ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

MINISTRY OF ECONOMY AND FINANCE

ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ
លេខ...៥៥៥១......សហវ....

ប្រកាស
ស្តីពី
ការដាក់ឱ្យប្រើប្រាស់ វិធាន និងនីតិវិធីនៃការចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា

ឧបនាយករដ្ឋមន្ត្រី រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ

- បានឃើញរដ្ឋធម្មនុញ្ញនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៩១៨/៩២៥ ចុះថ្ងៃទី០៦ ខែកញ្ញា ឆ្នាំ២០១៨ ស្តីពីការតែងតាំងរាជរដ្ឋាភិបាលនៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៣២០/៤១២ ចុះថ្ងៃទី៣០ ខែមីនា ឆ្នាំ២០២០ ស្តីពីការតែងតាំង និងកែសម្រួលសមាសភាពរាជរដ្ឋាភិបាល នៃព្រះរាជាណាចក្រកម្ពុជា
- បានឃើញព្រះរាជក្រឹត្យលេខ នស/រកត/០៨២១/៥៦៤ ចុះថ្ងៃទី៧ ខែសីហា ឆ្នាំ២០២១ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅរបស់ក្រុមប្រឹក្សាជាតិសេដ្ឋកិច្ចនិងសង្គមឌីជីថល
- បានឃើញព្រះរាជក្រមលេខ នស/រកម/០១៩៦/១៨ ចុះថ្ងៃទី២៥ ខែមករា ឆ្នាំ១៩៩៦ ដែលប្រកាសឱ្យប្រើច្បាប់ស្តីពីការបង្កើតក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ
- បានឃើញអនុក្រឹត្យលេខ ៧៥ អនក្រ.បក ចុះថ្ងៃទី២៥ ខែឧសភា ឆ្នាំ២០១៧ ស្តីពីការកែសម្រួលអនុក្រឹត្យលេខ ៤៨៨ ចុះថ្ងៃទី១៦ ខែតុលា ឆ្នាំ២០១៣ ស្តីពីការរៀបចំនិងប្រព្រឹត្តទៅនៃក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ
- បានឃើញអនុក្រឹត្យលេខ ២២០ អនក្រ.បក ចុះថ្ងៃទី១១ ខែវិច្ឆិកា ឆ្នាំ២០២១ ស្តីពីការរៀបចំនិងការប្រព្រឹត្តទៅរបស់គណៈកម្មាធិការសេដ្ឋកិច្ចនិងធុរកិច្ចឌីជីថល
- បានឃើញអនុក្រឹត្យលេខ ១៦៤ អនក្រ.បក ចុះថ្ងៃទី២៤ ខែសីហា ឆ្នាំ២០២១ ស្តីពីការផ្លាស់ប្តូរទិន្នន័យតាមរយៈថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា
- បានឃើញអនុក្រឹត្យលេខ ២៥២ អនក្រ.បក ចុះថ្ងៃទី២២ ខែធ្នូ ឆ្នាំ២០២១ ស្តីពីការគ្រប់គ្រងការប្រើប្រាស់ និងការការពារសុវត្ថិភាពទិន្នន័យអត្តសញ្ញាណបុគ្គល
- បានឃើញអនុក្រឹត្យលេខ ២៤៦ អនក្រ.បក ចុះថ្ងៃទី២៩ ខែធ្នូ ឆ្នាំ២០១៧ ស្តីពីហត្ថលេខាឌីជីថល
- យោងតាមតម្រូវការចាំបាច់របស់ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

សម្រេច

ប្រការ១.-

ដាក់ឱ្យប្រើប្រាស់ វិធាន និងនីតិវិធីនៃការចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា (**ថ.ផ.ទ.**) ដូចមានខ្លឹមសារភ្ជាប់មកជាមួយប្រកាសនេះ។ វិធាន និងនីតិវិធីនេះ អាចត្រូវបានធ្វើបច្ចុប្បន្នភាពតាមការចាំបាច់។

ប្រការ២.-

បទប្បញ្ញត្តិទាំងឡាយដែលផ្ទុយនឹងប្រកាសនេះ ត្រូវទុកជានិរាករណ៍។

ប្រការ៣.-

នាយកខុទ្ទកាល័យ អគ្គលេខាធិការ អគ្គនាយកនៃគ្រប់អគ្គនាយកដ្ឋាន អគ្គាធិការនៃអគ្គាធិការដ្ឋាន ប្រធានអង្គភាពពាក់ព័ន្ធក្រោមឱវាទក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ នាយកមជ្ឈមណ្ឌលបណ្តុះធុរកិច្ចថ្មី "តេជោ" និងគ្រប់សមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា ត្រូវទទួលបន្ទុកអនុវត្តប្រកាសនេះតាមភារកិច្ចរៀងៗខ្លួន ចាប់ពីថ្ងៃចុះហត្ថលេខានេះតទៅ។

ថ្ងៃព្រហស្បតិ៍ ១៤រោច ខែ អាសាឍ ឆ្នាំខាល ចត្វាស័ក ព.ស. ២៥៦៦
ធ្វើនៅរាជធានីភ្នំពេញ ថ្ងៃទី២៨ ខែ កក្កដា ឆ្នាំ២០២២

ឧបនាយករដ្ឋមន្ត្រី
រដ្ឋមន្ត្រីក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ

អគ្គបណ្ឌិតសភាចារ្យ **អូន ព័ន្ធមុនីរ័ត្ន**

កន្លែងទទួល÷
- ទីស្តីការគណៈរដ្ឋមន្ត្រី
- ខុទ្ទកាល័យសម្តេចអគ្គមហាសេនាបតីតេជោនាយករដ្ឋមន្ត្រី
- ខុទ្ទកាល័យសម្តេច ឯកឧត្តម លោកជំទាវឧបនាយករដ្ឋមន្ត្រី
    "ដើម្បីជូនជ្រាប"
- ដូចប្រការ៣
    "ដើម្បីអនុវត្ត"
- ឯកសារ កាលប្បវត្តិ

មាតិកា

ផ្នែកទី ១៖ សេចក្តីផ្តើម

ក. គោលបំណង

១. វិធាន និងនីតិវិធីនៃការចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា (**ថ.ផ.ទ.**) ត្រូវបានរៀបចំឡើងផ្អែកតាមស្មារតីនៃអនុក្រឹត្យ១៦៤ អនក្រ.បកចុះថ្ងៃទី២៤ ខែសីហា ឆ្នាំ២០២១ ស្តីពីការផ្លាស់ប្តូរទិន្នន័យតាមរយៈថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា ដោយកំណត់លម្អិតអំពីលក្ខខណ្ឌ និងកាតព្វកិច្ចរបស់សមាជិក **ថ.ផ.ទ.** ក្នុងការផ្លាស់ប្តូរទិន្នន័យក្នុងក្របខណ្ឌអន្តរប្រតិបត្តិការ ប្រកបដោយសុវត្ថិភាព តម្លាភាព និងគណនេយ្យភាព។

ខ. អ្នកប្រើប្រាស់ និងវិសាលភាពនៃការអនុវត្ត

២. វិធាន និងនីតិវិធីនេះ ត្រូវបានប្រើប្រាស់សម្រាប់ប្រតិបត្តិករ **ថ.ផ.ទ.** សមាជិក **ថ.ផ.ទ.** និងភាគីពាក់ព័ន្ធ ដើម្បីធានាឱ្យបាននូវនិរន្តរភាពនៃការប្រើប្រាស់ **ថ.ផ.ទ.** និងការការពារផលប្រយោជន៍របស់សមាជិក **ថ.ផ.ទ.** ។ វិធាន និងនីតិវិធីនេះ មានវិសាលភាពអនុវត្តចំពោះ រាល់ប្រតិបត្តិការផ្លាស់ប្តូរទិន្នន័យតាមរយៈ **ថ.ផ.ទ.** រវាងសមាជិក **ថ.ផ.ទ.** ដែលរួមមានសមាជិកដោយស្វ័យប្រវត្តិ និងសមាជិកដោយការស្នើសុំ។ ចំពោះការផ្លាស់ប្តូរទិន្នន័យពាក់ព័ន្ធនឹងវិស័យការពារជាតិ សន្តិសុខ និងសណ្តាប់ធ្នាប់សាធារណៈ ត្រូវអនុវត្តតាមលិខិតបទដ្ឋានគតិយុត្តពាក់ព័ន្ធក្នុងវិស័យការពារជាតិ សន្តិសុខ និងសណ្តាប់ធ្នាប់សាធារណៈជាធរមាន។

គ. ការធ្វើបច្ចុប្បន្នភាព "វិធាន និងនីតិវិធី" ចូលជាសមាជិក ថ.ផ.ទ.

៣. ប្រតិបត្តិករ **ថ.ផ.ទ.** ដែលមានក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ ជាអាណាព្យាបាលបច្ចេកទេស និងហិរញ្ញវត្ថុ ត្រូវពន្យល់ណែនាំ និងបកស្រាយអំពីវិធាន និងនីតិវិធីនេះ ជូនដល់សមាជិក **ថ.ផ.ទ.** និងត្រូវធ្វើបច្ចុប្បន្នភាពវិធាន និងនីតិវិធីនេះ ក្នុងពេលវេលាសមស្របតាមការចាំបាច់ ដើម្បីឆ្លុះបញ្ចាំងពីបទពិសោធន៍នៃការអនុវត្តជាក់ស្តែង និងឆ្លើយតបទៅនឹងការធ្វើវិសោធនកម្មច្បាប់ និងលិខិតបទដ្ឋានគតិយុត្តពាក់ព័ន្ធនានា។

ឃ. វាក្យសព្ទបច្ចេកទេស

៤. វាក្យសព្ទបច្ចេកទេសនៅក្នុងវិធាន និងនីតិវិធីនេះមានន័យដូចតទៅ៖

- **កូដនីយកម្ម** (Encryption) សំដៅដល់ការបំប្លែងព័ត៌មាន ឬទិន្នន័យទៅជាកូដពិសេសណាមួយដែលគេមិនអាចយល់ ឬប្រើប្រាស់បាន។
- **កំណត់ត្រាអេឡិចត្រូនិក** (Timestamp) សំដៅដល់កំណត់ត្រាដែលត្រូវបានបង្កើតឡើង ទាក់ទង ទទួល រក្សាទុក ឬដំណើរការក្នុងប្រព័ន្ធអេឡិចត្រូនិក ឬសម្រាប់បញ្ជូនពីប្រព័ន្ធអេឡិចត្រូនិកមួយទៅប្រព័ន្ធអេឡិចត្រូនិកមួយទៀត។
- **ចំនួនប្រតិបត្តិការ** (Number of transaction) សំដៅដល់ចំនួននៃការស្នើសុំទិន្នន័យមកកាន់អ្នកផ្តល់ទិន្នន័យ ដែលមួយប្រតិបត្តិការត្រូវបានកំណត់យកនៅពេលដែលអ្នកផ្តល់ទិន្នន័យឆ្លើយតបទៅវិញដោយជោគជ័យតាមតម្រូវការនៃការស្នើសុំទិន្នន័យនោះ។

- **ទិន្នន័យគោល** (Base registry) សំដៅដល់ទិន្នន័យមូលដ្ឋានដែលស្ថិតក្រោមការគ្រប់គ្រងរបស់ក្រសួង-ស្ថាប័នមានសមត្ថកិច្ចដែលជាម្ចាស់ទិន្នន័យដើម ហើយមានតែម្ចាស់ទិន្នន័យដើមទេដែលមានសិទ្ធិធ្វើបច្ចុប្បន្នភាពទិន្នន័យទាំងនោះស្របតាមច្បាប់និងលិខិតបទដ្ឋានគតិយុត្តជាធរមាន មានជាអាទិ៍ ទិន្នន័យអត្រានុកូលដ្ឋាន ទិន្នន័យបញ្ជាក់អត្តសញ្ញាណ (លិខិតឆ្លងដែន, បណ្ណបើកបរ, បណ្ណរបបសន្តិសុខសង្គម) ទិន្នន័យយានយន្ត ទិន្នន័យសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ ទិន្នន័យធុរកិច្ច ទិន្នន័យអចលនវត្ថុ ទិន្នន័យភូមិសាស្ត្រ ទិន្នន័យចំណូលសារពើពន្ធនិងមិនមែនសារពើពន្ធ ទិន្នន័យអប់រំ ទិន្នន័យការងារ ទិន្នន័យធានារ៉ាប់រង ទិន្នន័យរបបសន្តិសុខសង្គម ទិន្នន័យសុខាភិបាល និងទិន្នន័យរដ្ឋបាលថ្នាក់ក្រោមជាតិ។
- **ទិន្នន័យមូលដ្ឋាន** (Database) សំដៅដល់បណ្តុំនៃទំនាក់ទំនងទិន្នន័យ ឬព័ត៌មានដែលរក្សាទុកក្នុងកុំព្យូទ័រតាមវិធីណាមួយ ដោយក្នុងនោះ វាផ្តល់ភាពងាយស្រួលក្នុងការមើល បន្ថែម ស្វែងរក ឬធ្វើបច្ចុប្បន្នភាពទិន្នន័យ។
- **ម៉ាស៊ីនមេសុវត្ថិភាព** (Security server) សំដៅដល់ម៉ាស៊ីនមេដែលមានតួនាទីផ្ទៀងផ្ទាត់ការស្នើសុំឆ្លើយតប (request-response) របស់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានដែលធ្វើការផ្លាស់ប្តូរទិន្នន័យប្រកបដោយសុវត្ថិភាព ហើយមានតួនាទីជាអ្នកធ្វើកូដនីយកម្ម និងវិកូដនីយកម្មលើទិន្នន័យ។
- **ម្ចាស់ទិន្នន័យដើម** (Original data owner) សំដៅដល់ក្រសួង-ស្ថាប័នដែលមានសិទ្ធិអំណាចពេញលេញកាន់កាប់ទិន្នន័យជារបស់ខ្លួន និងដែលមានសមត្ថកិច្ចក្នុងការធ្វើបច្ចុប្បន្នភាពទិន្នន័យ។
- **យថាភូតភាព** (Authenticity) សំដៅដល់ការបញ្ជាក់អត្តសញ្ញាណអ្នកប្រើប្រាស់កុំព្យូទ័រក្នុងគោលបំណងសន្តិសុខ ដោយការផ្ទៀងផ្ទាត់ (ឈ្មោះ លេខសម្ងាត់ កាត ក្រយៅដៃ សំឡេង ភ្នែក មុខ ។ល។)។
- **វិធាន និងនីតិវិធី** (Rules and Procedures) សំដៅលើឯកសារនេះ និងឧបសម្ព័ន្ធដែលត្រូវបានគ្រប់គ្រងដោយច្បាប់នៃព្រះរាជាណាចក្រកម្ពុជា។ ប្រសិនបើវិធានណាមួយមានលក្ខណៈផ្ទុយនឹងច្បាប់ ឬបទប្បញ្ញត្តិនៃព្រះរាជាណាចក្រកម្ពុជា វិធាននោះត្រូវបាត់សុពលភាពអនុវត្តដោយមិនប៉ះពាល់ដល់សុពលភាពអនុវត្តនៃវិធានផ្សេងៗនោះទេ ហើយក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុនឹងធ្វើវិសោធនកម្មវិធាននោះឱ្យមានសុពលភាពអនុវត្តឡើងវិញ។
- **វិធាន** (Rules) សំដៅលើបញ្ញត្តិនីមួយៗនៃវិធាននិងនីតិវិធីនេះ។
- **សន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន** (Cyber security) សំដៅដល់បច្ចេកវិទ្យាប្រឆាំងនឹងការប្រើប្រាស់ទិន្នន័យព័ត៌មានដោយគ្មានការអនុញ្ញាត។
- **សន្ធានកម្មនៃកម្មវិធីកុំព្យូទ័រ** (Application Programming Interface **ឬហៅកាត់ថា** API) សំដៅដល់ច្រកចេញចូលស្តង់ដារដែលអនុញ្ញាតឱ្យទិន្នន័យអាចផ្លាស់ប្តូរពីប្រព័ន្ធបច្ចេកវិទ្យា

ព័ត៌មានមួយ ទៅប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានមួយផ្សេងទៀត។ ការផ្លាស់ប្តូរទិន្នន័យ គឺតម្រូវឱ្យស្របតាមលក្ខខណ្ឌដែលបានកំណត់។

- **សមាជិក (Member)** សំដៅលើសមាជិកដោយស្វ័យប្រវត្តិ និងសមាជិកដោយការស្នើសុំ ដែលសមាជិកនីមួយៗ អាចជាអ្នកទទួលទិន្នន័យ និង/ឬ ជាអ្នកផ្តល់ទិន្នន័យដែលត្រូវបានអនុញ្ញាតជាផ្លូវការឱ្យផ្លាស់ប្តូរទិន្នន័យ តាមរយៈថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា ។
- **ហត្ថលេខាឌីជីថល (Digital signature)** សំដៅដល់ទិន្នន័យ ដែលភ្ជាប់នឹងសារអេឡិចត្រូនិក ដើម្បីបញ្ជាក់អត្តសញ្ញាណនៃហត្ថលេខីឌីជីថល និងផ្ទៀងផ្ទាត់ស្ថានភាពដើមនៃសារអេឡិចត្រូនិក ដែលហត្ថលេខីឌីជីថលបានចុះហត្ថលេខា។

ផ្នែកទី២៖ សមាជិកភាព

ក. ប្រភេទនៃសមាជិក **ថ.ផ.ទ.**

៥. សមាជិក **ថ.ផ.ទ.** ត្រូវបានបែងចែកជាពីរប្រភេទរួមមាន៖ សមាជិកដោយស្វ័យប្រវត្តិ និងសមាជិកដោយការស្នើសុំ ដែលសមាជិកនីមួយៗអាចជាអ្នកទទួលទិន្នន័យ និង/ឬ ជាអ្នកផ្តល់ទិន្នន័យដូចមានចែងក្នុងមាត្រា៩ នៃអនុក្រឹត្យលេខ១៦៤ អនក្រ.បក ចុះថ្ងៃទី២៤ ខែសីហា ឆ្នាំ២០២១ ស្តីពីការផ្លាស់ប្តូរទិន្នន័យតាមរយៈថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា ។

៦. **សមាជិកដោយស្វ័យប្រវត្តិ** ជាវិស័យសាធារណៈដែលមានជាអាទិ៍ ក្រសួង ស្ថាប័ន អង្គភាពសាធារណៈប្រហាក់ប្រហែល គ្រឹះស្ថានសាធារណៈរដ្ឋបាល សហគ្រាសសាធារណៈ អង្គភាពស្វ័យភាពហិរញ្ញវត្ថុដទៃទៀត និងរដ្ឋបាលថ្នាក់ក្រោមជាតិ។

៧. **សមាជិកដោយការស្នើសុំ** ជាវិស័យឯកជនដែលមានជាអាទិ៍ ក្រុមហ៊ុន/សហគ្រាសពាណិជ្ជកម្ម សមាគម និងអង្គការមិនមែនរដ្ឋាភិបាល ដែលបានចុះបញ្ជីត្រឹមត្រូវស្របតាមច្បាប់ នៃព្រះរាជាណាចក្រកម្ពុជា។

ខ. លក្ខខណ្ឌជាក់លាក់សម្រាប់សមាជិក **ថ.ផ.ទ.**

៨. **សមាជិកដោយស្វ័យប្រវត្តិ** ត្រូវគោរពតាមលក្ខខណ្ឌជាក់លាក់ដូចខាងក្រោម៖

- រាល់ការផ្លាស់ប្តូរទិន្នន័យ ក្នុង**ក្របខណ្ឌទិន្នន័យគោល** ដើម្បីផ្តល់សេវាសាធារណៈ និងក្នុងក្របខណ្ឌអន្តរប្រតិបត្តិការនៃប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ត្រូវធ្វើឡើងនៅលើ **ថ.ផ.ទ.** តែមួយគត់
- ត្រូវសហការ និងសម្របសម្រួលជាមួយប្រតិបត្តិករ **ថ.ផ.ទ.** ក្នុងការរៀបចំបែបបទ និងនីតិវិធី ឬអនុស្សរណៈនៃការយោគយល់គ្នា សម្រាប់ការផ្លាស់ប្តូរទិន្នន័យលើ **ថ.ផ.ទ.** និងអាចមានការកែសម្រួលបែបបទ និងនីតិវិធី ឬអនុស្សរណៈនៃការយោគយល់គ្នា តាមការចាំបាច់ និង
- មិនតម្រូវឱ្យដាក់ពាក្យស្នើសុំចូលជាសមាជិកនោះទេ និងមិនអាចបោះបង់សមាជិកភាពបាននោះទេ វៀរលែងតែក្នុងករណីសមាជិកដោយស្វ័យប្រវត្តិនោះ ត្រូវបានរំលាយចោល ឬធ្វើសមាហរណកម្មជាមួយស្ថាប័នដទៃ ស្របទៅតាមច្បាប់ និងលិខិតបទដ្ឋានគតិយុត្តដែលមានជាធរមាន។

៩. **សមាជិកដោយការស្នើសុំ** ត្រូវគោរពតាមលក្ខខណ្ឌជាក់លាក់ដូចខាងក្រោម៖

- ត្រូវធានាថារាល់ការទទួលយក និងផ្លាស់ប្តូរទិន្នន័យ មិនផ្តល់ការគំរាមកំហែងដល់សន្តិសុខជាតិ មិនប៉ះពាល់ដល់ភាពស្របច្បាប់នៃផលប្រយោជន៍សាធារណៈ សណ្តាប់ធ្នាប់ និងផលប្រយោជន៍សង្គម សិទ្ធិឯកជនរបស់ម្ចាស់ទិន្នន័យ ឬប៉ះពាល់ដល់នយោបាយសាធារណៈរបស់រដ្ឋ
- ត្រូវធានាបានថា ទិន្នន័យដែលបានផ្លាស់ប្តូរតាមរយៈ **ថ.ផ.ទ.** ត្រូវបានប្រើប្រាស់ក្នុងគោលបំណងនៃការធ្វើធុរកិច្ច និងសង្គមកិច្ច ស្របតាមអនុស្សរណៈនៃការយោគយល់គ្នា ព្រមទាំងច្បាប់និងលិខិតបទដ្ឋានគតិយុត្តជាធរមាន
- ត្រូវធានាបាននូវគុណភាព និងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន
- ត្រូវមានហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ និងសម្ភារបរិក្ខារបច្ចេកវិទ្យាព័ត៌មានសមស្រប ដើម្បីបម្រុងសម្រាប់ប្រតិបត្តិការ ដោយធានានូវសន្តិសុខ សុវត្ថិភាព សុក្រឹតភាព និងគុណភាពប្រព័ន្ធ
- ត្រូវមានលទ្ធភាពដំឡើងម៉ាស៊ីនមេសុវត្ថិភាព ក្នុងបណ្តាញប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ខ្លួន
- ត្រូវមានសមត្ថភាព ចូលរួមសហការជាមួយក្រសួង-ស្ថាប័ន មានសមត្ថកិច្ចពាក់ព័ន្ធក្នុងការចាត់វិធានការឆ្លើយតប លើការវាយប្រហារប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន និង
- ត្រូវទទួលបន្ទុកចំណាយពាក់ព័ន្ធនឹងថ្លៃសមាជិកភាព។

គ. នីតិវិធីនៃការដាក់ពាក្យស្នើសុំចូលជាសមាជិក ថ.ផ.ទ.

១០. ដូចមានចែងក្នុងកថាខណ្ឌទី៨ នៃវិធាន និងនីតិវិធីនេះ, សមាជិកដោយស្វ័យប្រវត្តិ ដែលជាវិស័យសាធារណៈ មិនតម្រូវឱ្យដាក់ពាក្យស្នើសុំចូលជាសមាជិក **ថ.ផ.ទ.** នោះទេ ប៉ុន្តែត្រូវសហការជាមួយប្រតិបត្តិករ **ថ.ផ.ទ.** ក្នុងការរៀបចំអនុស្សរណៈនៃការយោគយល់គ្នា ឬបែបបទ និងនីតិវិធីសម្រាប់ការផ្លាស់ប្តូរទិន្នន័យលើ **ថ.ផ.ទ.** ។ អនុស្សរណៈនៃការយោគយល់គ្នា ត្រូវចុះហត្ថលេខារួមគ្នាដោយតំណាងក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ និងតំណាងសមាជិកដោយស្វ័យប្រវត្តិ។

១១. ដើម្បីអាចក្លាយជាសមាជិកដោយការស្នើសុំ, វិស័យឯកជន ត្រូវបំពេញពាក្យស្នើសុំ និងភ្ជាប់មកជាមួយនូវសំណុំឯកសារដូចខាងក្រោម៖

- ពាក្យស្នើសុំចូលជាសមាជិក ដែលត្រូវចុះហត្ថលេខាដោយនាយកប្រតិបត្តិ/ប្រធានស្ថាប័ន/អ្នកតំណាងស្របច្បាប់ ដូចមានភ្ជាប់ក្នុងឧបសម្ព័ន្ធ ១
- បញ្ជីរាយនាមបុគ្គលទំនាក់ទំនង និងក្រុមការងារបច្ចេកទេស និងធុរកិច្ច សម្រាប់រៀបចំការតភ្ជាប់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាននៅលើ **ថ.ផ.ទ.** និង
- ឯកសារចាំបាច់ ដែលអាចបញ្ជាក់ពីគុណវុឌ្ឍិគ្រប់គ្រាន់ ក្នុងការចូលជាសមាជិកដោយការស្នើសុំ ដូចបានកំណត់ក្នុងកថាខណ្ឌទី៩ នៃវិធាន និងនីតិវិធីនេះ។

១២. ប្រតិបត្តិករ **ថ.ផ.ទ.** នឹងពិនិត្យទៅលើសំណើសុំចូលជាសមាជិក និងគុណវុឌ្ឍិរបស់ស្ថាប័ន ដែលបានដាក់ពាក្យស្នើសុំ មុននឹងឆ្លើយតបជាផ្លូវការ។ សំណើសុំចូលជាសមាជិកដោយការស្នើសុំអាចត្រូវបានបដិសេធ ក្នុងករណីដែលពាក្យស្នើសុំចូលជាសមាជិក មិនបំពេញតាមលក្ខខណ្ឌដែលបាន

កំណត់ក្នុងវិធាន និងនីតិវិធីនេះ និងច្បាប់ និងលិខិតបទដ្ឋានគតិយុត្តជាធរមាន។ ប្រតិបត្តិករ **ថ.ផ.ទ.** អាចយល់ព្រម ឬបដិសេធ លើពាក្យស្នើសុំតាមឆន្ទានុសិទ្ធិរបស់ខ្លួន។

១៣. បន្ទាប់ពីទទួលបានលិខិតឯកភាពជាគោលការណ៍ពីប្រតិបត្តិករ **ថ.ផ.ទ.** ឱ្យចូលជាសមាជិកដោយការស្នើសុំ, ស្ថាប័នដែលដាក់ពាក្យស្នើសុំត្រូវបំពេញកាតព្វកិច្ចដូចខាងក្រោម៖

- រៀបចំផែនការសកម្មភាពសម្រាប់ការធ្វើសន្ទានកម្មនៃកម្មវិធីកុំព្យូទ័រ (Application Programming Interface-API)
- បំពេញតម្រូវការបច្ចេកទេស និងកាតព្វកិច្ចធ្វើតេស្តសាកល្បងដែលកំណត់ដោយប្រតិបត្តិករ **ថ.ផ.ទ.** និង
- រៀបចំការងារផ្សេងៗ តាមការកំណត់របស់ប្រតិបត្តិករ **ថ.ផ.ទ.** ។

១៤. ស្ថាប័នដាក់ពាក្យស្នើសុំ ដែលទទួលបានលិខិតឯកភាព ជាគោលការណ៍ពីប្រតិបត្តិករ **ថ.ផ.ទ.** ត្រូវអនុវត្តតាមលក្ខខណ្ឌតម្រូវ នៃលិខិតឯកភាពជាគោលការណ៍ ក្នុងរយៈពេលដែលបានកំណត់។ ក្នុងករណីចាំបាច់, ស្ថាប័នដែលដាក់ពាក្យស្នើសុំ អាចសុំពន្យារពេលជាផ្លូវការជាលាយលក្ខណ៍អក្សរមកប្រតិបត្តិករ **ថ.ផ.ទ.** ដើម្បីពន្យារពេលអនុវត្តកាតព្វកិច្ចដូចមានចែងក្នុងកថាខណ្ឌ១៣ នៃវិធាន និងនីតិវិធីនេះ ផ្អែកលើមូលហេតុច្បាស់លាស់ និងមិនបង្កផលប៉ះពាល់នានាដល់សមាជិក **ថ.ផ.ទ.** ដទៃទៀត។ ប្រតិបត្តិករ **ថ.ផ.ទ.** មានឆន្ទានុសិទ្ធិក្នុងការយល់ព្រម ឬបដិសេធ លើសំណើសុំពន្យារពេល។ ក្នុងករណីស្ថាប័នដាក់ពាក្យស្នើសុំ ដែលទទួលបានលិខិតឯកភាពជាគោលការណ៍ពីប្រតិបត្តិករ **ថ.ផ.ទ.** និងមិនអនុវត្តកាតព្វកិច្ចក្នុងរយៈពេលដែលបានកំណត់ ដោយមិនមានការស្នើសុំពន្យារពេល ឬជូនដំណឹងណាមួយ, ប្រតិបត្តិករ **ថ.ផ.ទ.** មានឆន្ទានុសិទ្ធិ ក្នុងការលុបចោលពាក្យស្នើសុំរបស់ស្ថាប័នដែលបានដាក់ពាក្យ។

ឃ. តម្រូវការបច្ចេកទេស

១៥. សមាជិកត្រូវគោរព និងអនុវត្តតាមឯកសារដូចខាងក្រោម៖

- ឯកសារណែនាំក្នុងការដំឡើងម៉ាស៊ីនសុវត្ថិភាព (Security Server Installation Guideline)
- ឯកសារណែនាំសម្រាប់ការប្រើប្រាស់ API និង API Catalog
- ឯកសារធានានូវគុណភាព និងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (Information Security Guideline) និង
- ឯកសារណែនាំសម្រាប់ការប្រើប្រាស់ប្រព័ន្ធវិក្កយបត្រនៃ **ថ.ផ.ទ.** (CamDX Billing System Guideline)។

ង. កាតព្វកិច្ចធ្វើតេស្ត

១៦. ប្រតិបត្តិករ **ថ.ផ.ទ.** អាចកំណត់អំពីវិធី និងកាលបរិច្ឆេទនៃការធ្វើតេស្ត ផ្អែកលើផែនការសកម្មភាពសម្រាប់ការធ្វើសន្ទានកម្មនៃកម្មវិធីកុំព្យូទ័រ (Application Programming Interface-API) ដែលសមាជិកបានដាក់ជូន ដើម្បីធានានូវប្រសិទ្ធភាពនៃដំណើរការប្រតិបត្តិការរវាងប្រព័ន្ធនិងប្រព័ន្ធ។

ប្រតិបត្តិករ **ថ.ផ.ទ.** នឹងផ្តល់ជូនសមាជិកនូវឯកសារធ្វើតេស្ត រួមមាន System Integrated Test (SIT) និង User Acceptance Test (UAT) ជូនដល់សមាជិក។ បន្ទាប់មក សមាជិកត្រូវរៀបចំផែនការធ្វើតេស្ត SIT និង UAT រួចជូនដំណឹងជាមុនមកប្រតិបត្តិករ ដើម្បីប្រតិបត្តិករ **ថ.ផ.ទ.** អាចពិនិត្យ និង/ឬ កែប្រែផែនការធ្វើតេស្តរបស់សមាជិក, ចូលរួមពិនិត្យការធ្វើតេស្ត និងទាមទារឱ្យមានការធ្វើតេស្ត សាជាថ្មីតាមការចាំបាច់។ ក្នុងករណីការធ្វើតេស្តទទួលបានជោគជ័យ សមាជិកត្រូវចុះហត្ថលេខាលើលិខិតទទួលស្គាល់ (Sign-off letter)។

ច. ការត្រៀមលក្ខណៈចាប់ផ្តើមផ្លាស់ប្តូរទិន្នន័យរបស់សមាជិក ថ.ផ.ទ.

១៧. ចំពោះសមាជិកដោយស្វ័យប្រវត្តិ ដែលមានគុណវុឌ្ឍិគ្រប់គ្រាន់, ប្រតិបត្តិករ **ថ.ផ.ទ.** ឬក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ នឹងផ្សព្វផ្សាយពីសមាជិកភាពជាផ្លូវការរបស់សមាជិក។

១៨. ចំពោះសមាជិកដោយការស្នើសុំ, ស្ថាប័នដែលបានដាក់ពាក្យស្នើសុំដែលទទួលបានលិខិតឯកភាពជាគោលការណ៍ពីប្រតិបត្តិករ **ថ.ផ.ទ.** និងបានបំពេញគ្រប់លក្ខខណ្ឌ ដែលបានកំណត់អាចស្នើសុំកាលបរិច្ឆេទមកកាន់ប្រតិបត្តិករ **ថ.ផ.ទ.** សម្រាប់ការធ្វើប្រតិបត្តិការផ្លាស់ប្តូរទិន្នន័យ។ ប្រតិបត្តិករ **ថ.ផ.ទ.** នឹងផ្សព្វផ្សាយពីសមាជិកភាពជាផ្លូវការជាសាធារណៈ។

១៩. សមាជិកទាំងពីរប្រភេទដែលអាចជាអ្នកផ្តល់ទិន្នន័យ និង/ឬ ជាអ្នកទទួលទិន្នន័យ ត្រូវធានាថារាល់នីតិវិធីនៃការផ្លាស់ប្តូរទិន្នន័យ ត្រូវបានអនុវត្តប្រកបដោយតម្លាភាព គណនេយ្យភាព និងអនុលោមតាមលក្ខខណ្ឌដូចបានកំណត់ ក្នុងអនុស្សរណៈនៃការយោគយល់គ្នា ឬកិច្ចសន្យា ឬលិខិតបទដ្ឋានគតិយុត្តដែលមានជាធរមាន ដោយគ្មានសមាជិកណាមួយ មានសិទ្ធិអនុម័ត ឬរក្សាវិធានណាមួយដែលប្រាសចាកនឹងលក្ខខណ្ឌដែលបានកំណត់នោះឡើយ។ រាល់ការធ្វើបច្ចុប្បន្នភាព ឬការកែប្រែលក្ខខណ្ឌណាមួយនៃនីតិវិធីក្នុងការផ្លាស់ប្តូរទិន្នន័យ, សមាជិកនីមួយៗ ត្រូវជូនដំណឹងមកប្រតិបត្តិករ **ថ.ផ.ទ.** ដើម្បីសម្របសម្រួល។ ប្រសិនបើសមាជិកណាមួយ ដែលជាអ្នកផ្តល់ទិន្នន័យ បដិសេធការផ្លាស់ប្តូរទិន្នន័យ សមាជិកនោះត្រូវផ្តល់ឱ្យសមាជិកដែលជាអ្នកស្នើសុំទិន្នន័យ(អ្នកទទួលទិន្នន័យ) នូវការពន្យល់ពីមូលហេតុ នៃការបដិសេធក្នុងរយៈពេលសមស្រប បន្ទាប់ពីមានការសម្របសម្រួលពីប្រតិបត្តិករ **ថ.ផ.ទ.**។

ឆ. ការបញ្ចប់សមាជិកភាព

២០. យោងតាមមាត្រា១៤ នៃអនុក្រឹត្យ១៦៤ អនក្រ.បកចុះថ្ងៃទី២៤ ខែសីហា ឆ្នាំ២០២១ ស្តីពីការផ្លាស់ប្តូរទិន្នន័យតាមរយៈថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា និងកថាខណ្ឌទី៨ នៃវិធាន និងនីតិវិធីនេះ, សមាជិកដោយស្វ័យប្រវត្តិ មិនអាចបោះបង់សមាជិកភាពទេ វៀរលែងតែក្នុងករណីដែលសមាជិកដោយស្វ័យប្រវត្តិនោះ ត្រូវបានរំលាយចោល ឬត្រូវបានធ្វើសមាហរណកម្មជាមួយស្ថាប័នដទៃ ស្របតាមច្បាប់និងលិខិតបទដ្ឋានគតិយុត្តជាធរមាន។

២១. ការបញ្ចប់សមាជិកភាពនេះធ្វើឡើងសម្រាប់តែសមាជិកដោយការស្នើសុំ និងធ្វើឡើងក្នុងរូបភាពចំនួន ០២ (ពីរ)៖

ក. **ការបញ្ចប់សមាជិកភាពតាមការស្នើសុំ៖** សមាជិកដោយការស្នើសុំ ដែលមានបំណងចង់បោះបង់សមាជិកភាពពី **ថ.ផ.ទ.** ត្រូវស្នើសុំជាលាយលក្ខណ៍អក្សរមកកាន់ប្រតិបត្តិករ **ថ.ផ.ទ.** ដោយមានហេតុផល និងអំណះអំណាងច្បាស់លាស់ ព្រមទាំងភ្ជាប់មកជាមួយនូវព័ត៌មានពាក់ព័ន្ធដូចជាការបំពេញពាក្យ និងបង់ថ្លៃពាក្យស្នើសុំបញ្ចប់សមាជិកភាពពី **ថ.ផ.ទ.** ដូចមានភ្ជាប់ក្នុងឧបសម្ព័ន្ធ៣។ ប្រតិបត្តិករ **ថ.ផ.ទ.** ត្រូវសម្របសម្រួលពីនីតិវិធីបោះបង់សមាជិកភាព និងជូនព័ត៌មានទៅកាន់សមាជិកដទៃទៀត ជាពិសេសសមាជិកពាក់ព័ន្ធ ដែលជាអ្នកទទួលទិន្នន័យ និង/ឬម្ចាស់ទិន្នន័យដើម។ ការបញ្ចប់សមាជិកភាពពី **ថ.ផ.ទ.** ត្រូវមានប្រសិទ្ធភាព គិតចាប់ពីថ្ងៃទទួលបានសេចក្តីជូនដំណឹង ស្តីពីការបញ្ចប់សមាជិកភាព ជាស្ថាពរដែលចេញដោយប្រតិបត្តិករ **ថ.ផ.ទ.**។

ខ. **ការបញ្ចប់សមាជិកភាពតាមសេចក្តីសម្រេចរបស់ប្រតិបត្តិករ ថ.ផ.ទ.** ៖ ប្រតិបត្តិករ **ថ.ផ.ទ.** មានសិទ្ធិពេញលេញ ក្នុងការបញ្ចប់សមាជិកភាពរបស់សមាជិកដោយការស្នើសុំណាមួយ ក្នុងករណីរកឃើញថា សមាជិកនោះបានប្រព្រឹត្តមិនប្រក្រតី ឬមិនគោរពតាមគោលការណ៍ ឬលក្ខខណ្ឌណាមួយដែលមានចែងក្នុងកិច្ចសន្យា ឬ អនុស្សរណៈនៃការយោគយល់គ្នា ជាមួយប្រតិបត្តិករ ឬបានប្រព្រឹត្តល្មើសនឹងច្បាប់ និងលិខិតបទដ្ឋានគតិយុត្តជាធរមាន, ឬក្នុងករណីសមាជិកបង្កឱ្យមានផលប៉ះពាល់ធ្ងន់ធ្ងរ ឬគំរាមកំហែងដល់ **ថ.ផ.ទ.** ឬដល់សមាជិកដទៃទៀត ឬ សាធារណជន។ នីតិវិធីនៃការបញ្ចប់សមាជិកភាពតាមសេចក្តីសម្រេចរបស់ប្រតិបត្តិករ **ថ.ផ.ទ.** ត្រូវរៀបចំតាមនីតិវិធីដូចមានចែងក្នុងឧបសម្ព័ន្ធ ៤។

ផ្នែកទី៣៖ តួនាទី និងការទទួលខុសត្រូវ

ក. តួនាទី និងការទទួលខុសត្រូវរបស់ប្រតិបត្តិករ ថ.ផ.ទ.

២២. ប្រតិបត្តិករ **ថ.ផ.ទ.** មានតួនាទី*គ្រប់គ្រង*ប្រតិបត្តិការរបស់ **ថ.ផ.ទ.** ដែលមានក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុជាអាណាព្យាបាលបច្ចេកទេស និងហិរញ្ញវត្ថុ។ បន្ថែមលើតួនាទីជាអ្នកគ្រប់គ្រងប្រតិបត្តិការរបស់ **ថ.ផ.ទ.**, ប្រតិបត្តិករ **ថ.ផ.ទ.** មានតួនាទីជាអ្នក*ត្រួតពិនិត្យ*ការផ្លាស់ប្តូរទិន្នន័យលើ **ថ.ផ.ទ.** របស់សមាជិក **ថ.ផ.ទ.** ដើម្បីធានាថារាល់ការផ្លាស់ប្តូរទិន្នន័យតាមរយៈ **ថ.ផ.ទ.** ទិន្នន័យមិនត្រូវបានរក្សាទុក នៅក្នុងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ **ថ.ផ.ទ.** និង/ឬ ចែកចាយជាមួយរូបវន្តបុគ្គល ឬនីតិបុគ្គលណាមួយ ដោយគ្មានការអនុញ្ញាតពីម្ចាស់ទិន្នន័យដើមទេ និងមានតួនាទីបន្ថែមទៀតដូចខាងក្រោម៖

- ថែរក្សា និងធ្វើបច្ចុប្បន្នភាព **ថ.ផ.ទ.** តាមការចាំបាច់
- ទទួលយក ឬបដិសេធ សំណើសុំចូលជាសមាជិកដោយការស្នើសុំ ឬពង្រីកវិសាលភាពនៃការទទួលយកសមាជិកភាព

- ចេញផ្សាយលិខិតបទដ្ឋានគតិយុត្តពាក់ព័ន្ធ ឬឯកសារផ្សេងៗ ដើម្បីឱ្យសមាជិកអនុវត្តតាមគោលការណ៍ ឬលក្ខខណ្ឌដែលបានកំណត់
- បញ្ចប់សមាជិកភាពនៃសមាជិកណាមួយ ដូចបានកំណត់ក្នុងកថាខណ្ឌទី២១ នៃវិធាន និងនីតិវិធីនេះ
- រៀបចំវិធាន និងនីតិវិធីនៃការកំណត់កម្រៃសេវា ពាក់ព័ន្ធនឹងការផ្លាស់ប្តូរទិន្នន័យ សម្រាប់សមាជិក **ថ.ផ.ទ.**
- ត្រូវរៀបចំឱ្យមានការត្រួតពិនិត្យ វាយតម្លៃ លើសន្តិសុខប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ **ថ.ផ.ទ.** តាមការចាំបាច់ដោយស្ថាប័នជំនាញ និងមានកាតព្វកិច្ច អនុវត្តតាមរបាយការណ៍ត្រួតពិនិត្យ វាយតម្លៃ និងធ្វើការជួសជុលចំណុចខ្វះខាត ដែលអាចគំរាមកំហែងដល់សន្តិសុខប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ **ថ.ផ.ទ.**
- ធ្វើវិសោធនកម្មវិធាន និងនីតិវិធីនេះតាមការចាំបាច់
- សម្របសម្រួលដោះស្រាយបញ្ហា ឬវិវាទផ្សេងៗ ដែលអាចកើតមានរវាងសមាជិក និងសមាជិក
- បំពេញភារកិច្ចផ្សេងៗ តាមការកំណត់របស់ក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ ដែលជាអាណាព្យាបាលបច្ចេកទេស និងហិរញ្ញវត្ថុ។

ខ. តួនាទី និងការទទួលខុសត្រូវរបស់សមាជិក ថ.ផ.ទ.

២៣. សមាជិក **ថ.ផ.ទ.** ទាំងពីរប្រភេទត្រូវ មានតួនាទី និងភារកិច្ចដូចតទៅ៖

- ផ្លាស់ប្តូរ និងប្រើប្រាស់ទិន្នន័យ ស្របតាមវិធាន និងនីតិវិធីដូចមានចែងក្នុងលិខិតបទដ្ឋានគតិយុត្ត ជាធរមាន ឬអនុស្សរណៈនៃការយោគយល់គ្នា ជាមួយក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ ឬជាមួយប្រតិបត្តិករ **ថ.ផ.ទ.**
- ត្រូវសហការជាមួយប្រតិបត្តិករ **ថ.ផ.ទ.** ដើម្បីរៀបចំឱ្យមានការត្រួតពិនិត្យ វាយតម្លៃលើសន្តិសុខប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ **ថ.ផ.ទ.** តាមការចាំបាច់ដោយស្ថាប័នជំនាញ
- រៀបចំធ្វើយថាភូតភាពអត្តសញ្ញាណឌីជីថល ជាមួយប្រព័ន្ធផ្ទៀងផ្ទាត់អត្តសញ្ញាណរួមរបស់ **ថ.ផ.ទ.** ដើម្បីកំណត់អត្តសញ្ញាណសមាជិកនៅពេលផ្លាស់ប្តូរទិន្នន័យ
- ទទួលខុសត្រូវថែទាំហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ និងបច្ចេកទេសរបស់ខ្លួន តាមការតម្រូវរបស់ប្រតិបត្តិករ **ថ.ផ.ទ.**
- រាយការណ៍ជូនប្រតិបត្តិករ រាល់ភាពមិនប្រក្រតីលើការផ្លាស់ប្តូរទិន្នន័យតាម **ថ.ផ.ទ.** ក្នុងរយៈពេលមិនលើសពី ២៤ (ម្ភៃបួន) ម៉ោង ក្រោយពីបានវាយតម្លៃរួច
- ចងក្រង រក្សាទុករបាយការណ៍ និងឯកសារពាក់ព័ន្ធនឹងការផ្លាស់ប្តូរទិន្នន័យតាមរយៈ **ថ.ផ.ទ.**
- រៀបចំ និងថែរក្សាកំណត់ត្រាបច្ចេកទេស ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ខ្លួន ដើម្បីជាមូលដ្ឋាន ក្នុងការត្រួតពិនិត្យសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន

- សហការដោះស្រាយរាល់បញ្ហានានា ពាក់ព័ន្ធនឹងប្រតិបត្តិការ **ថ.ផ.ទ.** ឱ្យបានឆាប់បំផុត
- ផ្តល់កិច្ចសហការផ្សេងទៀតតាមការស្នើសុំរបស់ប្រតិបត្តិករ **ថ.ផ.ទ.** និង/ឬ ក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ ទាក់ទងនឹងការផ្លាស់ប្តូរទិន្នន័យតាម **ថ.ផ.ទ.** និង
- ត្រូវទទួលខុសត្រូវ លើបន្ទុកចំណាយប្រតិបត្តិការតភ្ជាប់ ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ខ្លួនមកកាន់ **ថ.ផ.ទ.** ដែលមានជាអាទិ៍ ហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ សម្ភារបរិក្ខារអេឡិចត្រូនិក និងធនធានមនុស្ស ។

ផ្នែកទី៤៖ យន្តការសុវត្ថិភាព

២៤. ទិន្នន័យដែលត្រូវផ្លាស់ប្តូរតាមរយៈ **ថ.ផ.ទ.** ត្រូវបានធ្វើកូដនីយកម្ម និងចុះហត្ថលេខាឌីជីថល ដើម្បីធានាបាននូវសុវត្ថិភាព សុចរិតភាព និងសុក្រឹត្យភាពនៃទិន្នន័យ ព្រមទាំងត្រូវបានធ្វើកំណត់ត្រាអេឡិចត្រូនិកពីការផ្លាស់ប្តូរទិន្នន័យ។

២៥. ប្រតិបត្តិករ **ថ.ផ.ទ.** មានកាតព្វកិច្ចអនុវត្តតាមរបាយការណ៍ត្រួតពិនិត្យ វាយតម្លៃ និងធ្វើការជួសជុលចំណុចខ្វះខាត ដែលអាចគំរាមកំហែងដល់សន្តិសុខប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ **ថ.ផ.ទ.** បន្ទាប់ពីទទួលបានការត្រួតពិនិត្យ និងវាយតម្លៃពីស្ថាប័នជំនាញតាមការចាំបាច់។

២៦. ដើម្បីធានាសុវត្ថិភាព និងប្រសិទ្ធភាពប្រតិបត្តិការនៅលើ **ថ.ផ.ទ.**, រាល់សមាជិក **ថ.ផ.ទ.** ត្រូវអនុវត្តដូចខាងក្រោម៖

- ត្រូវមានវិធានការសន្តិសុខ តាមប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរៀងៗខ្លួន ក្នុងការការពារ និងទប់ស្កាត់ការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិត ទៅលើប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានរបស់ខ្លួន ដែលប៉ះពាល់ដល់ប្រក្រតីភាពនៃដំណើរការផ្លាស់ប្តូរទិន្នន័យលើ **ថ.ផ.ទ.** និងទិន្នន័យផ្ទាល់ខ្លួនរបស់ឯកជន ដែលការពារដោយច្បាប់
- ត្រូវរាយការណ៍ជូនប្រតិបត្តិករ **ថ.ផ.ទ.** ពីហានិភ័យដែលអាចបង្កឡើង និង/ឬប៉ះពាល់ដល់សុវត្ថិភាព **ថ.ផ.ទ.** និងត្រូវសហការជាមួយប្រតិបត្តិករ **ថ.ផ.ទ.** ដើម្បីរកដំណោះស្រាយ
- ត្រូវរៀបចំយន្តការត្រួតពិនិត្យផ្ទៃក្នុង ដែលមានប្រសិទ្ធភាព និងត្រូវរៀបចំឱ្យមានការត្រួតពិនិត្យ និងវាយតម្លៃ លើសន្តិសុខប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន តាមការចាំបាច់ដោយស្ថាប័នជំនាញ
- រៀបចំប្រព័ន្ធប្រតិបត្តិការសុវត្ថិភាពឱ្យបានរឹងមាំ ដើម្បីរក្សានូវជំនឿទុកចិត្តរបស់អ្នកប្រើប្រាស់ជាពិសេសរាល់ប្រតិបត្តិការនៅលើ **ថ.ផ.ទ.**
- មានធនធានមនុស្ស និងឧបករណ៍បច្ចេកទេសគ្រប់គ្រាន់ សម្រាប់ដំណើរការប្រព័ន្ធឱ្យមានសុវត្ថិភាព និងប្រសិទ្ធភាព
- រៀបចំផែនការសង្គ្រោះបន្ទាន់ រួមទាំងមធ្យោបាយសម្រាប់រក្សា និងសង្គ្រោះទិន្នន័យ កុំឱ្យបាត់បង់ និង

- រៀបចំយន្តការតាមដាន និងទប់ស្កាត់ប្រតិបត្តិការក្លែងបន្លំ ព្រមទាំងយុទ្ធសាស្ត្រក្នុងការកំណត់ និងបង្ការហានិភ័យ និង/ឬយន្តការសុវត្ថិភាពផ្សេងៗទៀត ដែលកំណត់ដោយប្រតិបត្តិករ **ថ.ផ.ទ.** តាមការចាំបាច់។

២៧. សមាជិក **ថ.ផ.ទ.** ត្រូវធានាថា ប្រព័ន្ធរបស់ខ្លួនប្រព្រឹត្តទៅដោយសុវត្ថិភាពខ្ពស់ ហើយមិនអាចធ្វើឱ្យប៉ះពាល់ដល់ប្រព័ន្ធដទៃនៅលើ **ថ.ផ.ទ.** ។ ក្នុងករណីប្រព័ន្ធរបស់សមាជិក **ថ.ផ.ទ.** ណាមួយ មានបញ្ហា (ភាគីបង្ក) ដោយមិនបានគោពតាមវិធាន និងនីតិវិធីនេះ ឬតាមការណែនាំរបស់ប្រតិបត្តិករ **ថ.ផ.ទ.** ឬមានបញ្ហាណាមួយ ដែលបង្កផលប៉ះពាល់ដល់ប្រព័ន្ធរបស់សមាជិកដទៃ (ភាគីរងការប៉ះពាល់), ភាគីបង្ក ត្រូវទទួលខុសត្រូវចំពោះការខាតបង់ និង/ឬ បន្ទុកដោះស្រាយបញ្ហា។

ផ្នែកទី៥៖ ការការពារផលប្រយោជន៍របស់សមាជិក ថ.ផ.ទ.

២៨. សមាជិក **ថ.ផ.ទ.** ដែលជាម្ចាស់ទិន្នន័យដើម អាចកំណត់កម្រៃសេវា ក្នុងមួយប្រតិបត្តិការនៃការទាញយកទិន្នន័យពីសមាជិក **ថ.ផ.ទ.** ដែលជាអ្នកទទួលទិន្នន័យ ទៅតាមប្រភេទនៃទិន្នន័យ ដោយត្រូវគោរពតាមវិធាន និងនីតិវិធីដែលកំណត់ដោយលិខិតបទដ្ឋានគតិយុត្តដោយឡែក។

ផ្នែកទី៦៖ ស្ថានភាពគ្រោះអាសន្ន

២៩. ប្រព័ន្ធរបស់សមាជិក ដែលមានប្រតិបត្តិការនៅលើ **ថ.ផ.ទ.** អាចប្រឈមនឹងការផ្អាកប្រតិបត្តិការក្នុងករណីដូចខាងក្រោម៖

- ករណីប្រធានសក្តិ
- ដាច់ចរន្តអគ្គិសនី
- ដាច់បណ្តាញទំនាក់ទំនងដោយប្រការណាមួយ និង/ឬ
- គ្រោះអាសន្នផ្សេងៗដែលជាឧបសគ្គ ក្នុងដំណើរការរបស់ប្រព័ន្ធនៅលើ **ថ.ផ.ទ**

៣០. ក្នុងការទប់ស្កាត់ហានិភ័យក៏ដូចជាគ្រប់គ្រងស្ថានការណ៍ខាងលើនេះ សមាជិកទាំងអស់ត្រូវកំណត់ឱ្យបានច្បាស់លាស់ នូវជម្រើសនៃការអនុវត្តវិធានសង្គ្រោះ និងយុទ្ធសាស្ត្រនានា ដើម្បីរក្សានូវដំណើរការប្រតិបត្តិការរបស់ប្រព័ន្ធទាំងមូល។

ផ្នែកទី៧៖ ការដោះស្រាយបញ្ហាបច្ចេកទេស

៣១. ក្នុងករណីសមាជិកណាមួយមានបញ្ហាបច្ចេកទេស ឬពិនិត្យឃើញនូវភាពមិនប្រក្រតីលើការផ្លាស់ប្តូរទិន្នន័យតាម **ថ.ផ.ទ.**, សមាជិកនោះត្រូវរាយការណ៍មកប្រតិបត្តិករ **ថ.ផ.ទ.** ក្នុងរយៈពេលមិនលើសពី ២៤ (ម្ភៃបួន) ម៉ោង ដើម្បីកំណត់ពីបញ្ហា និងស្វែងរកដំណោះស្រាយ។ រាល់ការចំណាយទៅលើការដោះស្រាយបញ្ហាបច្ចេកទេស នៃប្រព័ន្ធរបស់សមាជិកពាក់ព័ន្ធនឹងប្រតិបត្តិការ នៅលើ **ថ.ផ.ទ.** គឺជាបន្ទុករបស់សមាជិក និងអាចមានការសម្របសម្រួលពីប្រតិបត្តិករ **ថ.ផ.ទ.** តាមការចាំបាច់ ។

ផ្នែកទី៨៖ ការដោះស្រាយវិវាទ

៣២. ប្រតិបត្តិករ **ថ.ផ.ទ.** ត្រូវបង្កើតឱ្យមានយន្តការអព្យាក្រឹតមួយ សម្រាប់ទទួល និងសម្រុះសម្រួលដោះស្រាយវិវាទរបស់សមាជិក **ថ.ផ.ទ.** ពាក់ព័ន្ធនឹងការផ្លាស់ប្តូរទិន្នន័យនៅលើ **ថ.ផ.ទ.**។ ក្នុងវិធាន និងនីតិវិធីនេះ, **បណ្តឹង** សំដៅដល់ការតវ៉ា ឬការទាមទារ ឬការមិនពេញចិត្ត ដែលពាក់ព័ន្ធនឹងការផ្លាស់ប្តូរទិន្នន័យនៅលើ **ថ.ផ.ទ.**, **ការសម្រុះសម្រួលដោះស្រាយបណ្តឹង ឬវិវាទ** សំដៅដល់ដំណើរការ នៃការស្វែងរកដំណោះស្រាយមួយសមស្រប ដោយអនុលោមតាមច្បាប់និងលិខិតបទដ្ឋានគតិយុត្តជាធរមាន និង **ការស៊ើបអង្កេត** សំដៅដល់ដំណើរការស្រាវជ្រាវ ស្វែងរកភស្តុតាងដើម្បីបញ្ជាក់ការពិត ឬមិនពិត ចំពោះអង្គហេតុដូចមាននៅក្នុងពាក្យបណ្តឹង។

៣៣. ប្រតិបត្តិករ **ថ.ផ.ទ.** មានសិទ្ធិក្នុងការស៊ើបអង្កេតបណ្តឹង ពាក់ព័ន្ធនឹងការផ្លាស់ប្តូរទិន្នន័យ នៅលើ **ថ.ផ.ទ.** ឬអាចផ្តល់របាយការណ៍ ព័ត៌មាន ឬទិន្នន័យ ពាក់ព័ន្ធនឹងប្រតិបត្តិការដែលជាកម្មវត្ថុនៃបណ្តឹង ឬវិវាទក្នុងអំឡុងពេលដោះស្រាយបណ្តឹង ឬវិវាទតាមការស្នើសុំរបស់សមាជិក **ថ.ផ.ទ.** ប៉ុន្តែពុំមានសិទ្ធិចេញសេចក្តីសម្រេច ដើម្បីចាត់វិធានការដោះស្រាយ ឬដាក់ទណ្ឌកម្មឡើយ។ ប្រតិបត្តិករ **ថ.ផ.ទ.** អាចស្នើសុំកិច្ចសហការ ឬការចូលរួមពីសមាជិកពាក់ព័ន្ធ ឬអង្គភាពពាក់ព័ន្ធនានា ក្នុងការដោះស្រាយវិវាទតាមការចាំបាច់។ ក្នុងករណីបណ្តឹង ឬវិវាទមិនអាចសម្រុះសម្រួលដោះស្រាយបាន, ប្រតិបត្តិករ **ថ.ផ.ទ.** ត្រូវរាយការណ៍ជូនក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ ដែលជាអាណាព្យាបាលបច្ចេកទេស និងហិរញ្ញវត្ថុ ដើម្បីដោះស្រាយបន្ត ឬបញ្ជូនបន្តទៅកាន់ស្ថាប័នមានសមត្ថកិច្ចនៃព្រះរាជាណាចក្រកម្ពុជា ផ្អែកលើនីតិវិធីច្បាប់ជាធរមាន។

ផ្នែកទី៩៖ វិធានទូទៅ

៣៤. វិធាន និងនីតិវិធីនេះត្រូវបានធ្វើឡើងជាភាសាខ្មែរ។ ក្នុងករណីមានការបកប្រែ ហើយមានខ្លឹមសារផ្ទុយគ្នារវាងឯកសារជាភាសាខ្មែរ និងភាសាដែលបកប្រែ ខ្លឹមសារនៅក្នុងភាសាខ្មែរត្រូវមានអានុភាពអនុវត្ត។

៣៥. រាល់ការទំនាក់ទំនង ត្រូវធ្វើឡើងដោយប្រើប្រាស់ព័ត៌មានទំនាក់ទំនង ដែលផ្តល់ឱ្យដោយសមាជិក **ថ.ផ.ទ.** ដូចបានកំណត់ក្នុងវិធាន និងនីតិវិធីនេះ ឬតាមការជូនដំណឹងរបស់ប្រតិបត្តិករ **ថ.ផ.ទ.** ។ ចំពោះការធ្វើបច្ចុប្បន្នភាពព័ត៌មានទំនាក់ទំនង សមាជិកត្រូវជូនដំណឹងជាមុនមក ប្រតិបត្តិករ **ថ.ផ.ទ.**។

ឧបសម្ព័ន្ធ១៖ ពាក្យស្នើសុំចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា

ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ពាក្យស្នើសុំចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា

សូមគោរពជូន
ឯកឧត្តមនាយក មជ្ឈមណ្ឌលបណ្តុះធុរកិច្ចថ្មី "តេជោ"

កម្មវត្ថុ ៖ សំណើសុំចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា។

សេចក្តីដូចមានចែងក្នុងកម្មវត្ថុខាងលើ ខ្ញុំសូមគោរពជម្រាបជូន **ឯកឧត្តមនាយក** មេត្តាជ្រាបថា៖ ឈ្មោះអង្គភាពស្នើសុំ:..ជាអក្សរឡាតាំង:..................................ប្រភេទអង្គភាព/ក្រុមហ៊ុន:
....តំណាងដោយ(ឈ្មោះអ្នកតំណាងស្របច្បាប់របស់អង្គភាព/ក្រុមហ៊ុន):............

....□អត្តសញ្ញាណប័ណ្ណ/□លិខិតឆ្លងដែនលេខ:...

លេខទូរស័ព្ទ:..........................លេខទូរសារ:.........................អ៊ីម៉ែល:...

អាសយដ្ឋានបច្ចុប្បន្ន:..

មានបំណងចូលជា សមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា និងយល់ព្រមទទួលយកនូវគ្រប់លក្ខខណ្ឌ និងការអនុវត្តភារកិច្ចដូចមានចែងក្នុង "វិធាន និងនីតិវិធីនៃការចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា" ។

សូមគោរពភ្ជាប់មកជាមួយនូវ៖

- លិខិតផ្ទេរសិទ្ធិ (ក្នុងករណី អ្នកតំណាងមិនមែននាយកប្រតិបត្តិឬប្រធានស្ថាប័ន)
- បញ្ជីរាយនាមបុគ្គលទំនាក់ទំនង និងក្រុមការងារបច្ចេកទេសនិងធុរកិច្ច សម្រាប់រៀបចំការតភ្ជាប់ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាននៅលើ **ថ.ផ.ទ.** និង
- ឯកសារចាំបាច់ដែលអាចបញ្ជាក់ពីគុណវុឌ្ឍិគ្រប់គ្រាន់ក្នុងការចូលជាសមាជិក **ថ.ផ.ទ.** ។

ខ្ញុំសូមធានាអះអាង៖

- រាល់ព័ត៌មានទាំងអស់ដែលបានបំពេញនៅក្នុងពាក្យស្នើសុំនេះ ពិត និង ត្រឹមត្រូវ
- ពាក្យស្នើសុំត្រូវបានធ្វើឡើងក្នុងដែនសមត្ថកិច្ចរបស់អង្គភាពស្នើសុំ
- បានផ្តល់ឯកសារពាក់ព័ន្ធ និងគោរពតាមរាល់លក្ខខណ្ឌដូចមានកំណត់ក្នុង "វិធាន និងនីតិវិធីនៃការចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា" ។

អាស្រ័យដូចបានគោរពជម្រាបជូនខាងលើ, សូម **ឯកឧត្តមនាយក** មេត្តាអនុញ្ញាតតាមការស្នើសុំដោយក្តីអនុគ្រោះ។

ថ្ងៃ..........................ខែ...........ឆ្នាំ..........ព.ស.............
រាជធានីភ្នំពេញ ថ្ងៃទី......... ខែ.............ឆ្នាំ.............
នាយកប្រតិបត្តិ/ប្រធានស្ថាប័ន/អ្នកតំណាងស្របច្បាប់

ឧបសម្ព័ន្ធ២៖ កិច្ចសន្យាស្តីពីការទទួលយក និងការអនុវត្តតាម "វិធាន និងនីតិវិធីនៃការចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា"

កិច្ចសន្យា
ស្តីពី
ការទទួលយក និងការអនុវត្តតាម
"វិធាន និងនីតិវិធីនៃការចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា"

មជ្ឈមណ្ឌលបណ្តុះធុរកិច្ចថ្មី "**តេជោ**" ដែលជាប្រតិបត្តិករ **ថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា** មានទីតាំងស្ថិតនៅជាន់ទី១១ នៃមជ្ឈមណ្ឌលអភិវឌ្ឍធុរកិច្ច, មហាវិថីអូស៊ីអាយស៊ី សង្កាត់ជ្រោយចង្វារ ខណ្ឌជ្រោយចង្វារ រាជធានីភ្នំពេញ ព្រះរាជាណាចក្រកម្ពុជា តំណាងដោយ (ឈ្មោះ)..តួនាទី.................
....។

និង

....(ឈ្មោះអង្គភាព) អាសយដ្ឋាន...
....តំណាងដោយ(ឈ្មោះ)..
តួនាទី..តទៅនេះ ហៅថា "**សមាជិក ថ.ផ.ទ.**" ។

មជ្ឈមណ្ឌលបណ្តុះធុរកិច្ចថ្មី "**តេជោ**" **និង**..តទៅនេះ ហៅដាច់ដោយឡែកពីគ្នាថា "ភាគី" និងហៅរួមគ្នាថា "គូភាគី" បានព្រមព្រៀងគ្នាតាមលក្ខខណ្ឌខាងក្រោម៖

- ទទួលយក និងអនុវត្តតាមលក្ខខណ្ឌដែលបានចែងក្នុង "វិធាន និងនីតិវិធីចូលជាសមាជិកថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា"
- រក្សាស្តង់ដា និងសុវត្ថិភាពនៃប្រព័ន្ធរបស់សមាជិក ដើម្បីធានាឱ្យបាននូវនិរន្តរភាពនៃការប្រើប្រាស់ **ថ.ផ.ទ.**
- ទទួលខុសត្រូវ និងអនុវត្តឱ្យបានម៉ឺងម៉ាត់នូវកាតព្វកិច្ច និងភារកិច្ចរបស់ខ្លួន
- ដោះស្រាយវិវាទ ក្នុងករណីវិវាទបណ្តាលមកពីការអនុវត្តកិច្ចសន្យានេះ
- ចូលរួមដោះស្រាយបញ្ហាពាក់ព័ន្ធផ្សេងៗទៀត ដែលអាចកើតមានជាយថាហេតុ
- សមាជិក **ថ.ផ.ទ.** ត្រូវទទួលបន្ទុកចំណាយពាក់ព័ន្ធនឹងថ្លៃសមាជិកភាព។ ដោយឡែក ចំពោះកម្រៃសេវាពាក់ព័ន្ធនឹងប្រតិបត្តិការនៃការផ្លាស់ប្តូរទិន្នន័យ នឹងអនុវត្តតាមលិខិតបទដ្ឋានគតិយុត្តដោយឡែក។

ភាគីនៃកិច្ចសន្យា បានអាន បានស្តាប់ បានយល់ និងព្រមព្រៀងរាល់ខ្លឹមសារខាងលើ និងប្តេជ្ញាគោរពយ៉ាងម៉ឺងម៉ាត់រាល់លក្ខខណ្ឌដូចបានកំណត់។ ផ្ទុយទៅវិញ ប្រសិនបើភាគីណាមួយមិនគោរពតាមកិច្ចសន្យានេះ ភាគីនោះត្រូវទទួលខុសត្រូវចំពោះមុខច្បាប់ជាធរមាន។

កិច្ចសន្យានេះ ត្រូវបានធ្វើឡើងជាភាសាខ្មែរ ដែលគូភាគី អាចបកប្រែជាភាសាផ្សេងទៀតបាន។ ក្នុងករណីមានភាពមិនស្របគ្នារវាងខ្លឹមសារបកប្រែ នោះខ្លឹមសារជាភាសាខ្មែរ មានអានុភាពអនុវត្ត។ កិច្ចសន្យានេះ ត្រូវបានធ្វើឡើង និងចុះហត្ថលេខាជាសំណៅច្បាប់ដើមចំនួន ០២ (ពីរ) ច្បាប់ ដែលមានតម្លៃគតិយុត្តស្មើគ្នា ហើយគូភាគីត្រូវរក្សាទុកម្នាក់ ០១ (មួយ) ច្បាប់រៀងខ្លួន។

កិច្ចសន្យានេះធ្វើឡើងនៅ រាជធានីភ្នំពេញ ថ្ងៃ..................................ខែ............ឆ្នាំ..........ព.ស.............
ត្រូវនឹងថ្ងៃទី.........ខែ............ឆ្នាំ...........។

តំណាងសមាជិក	តំណាង **មជ្ឈមណ្ឌលបណ្តុះធុរកិច្ចថ្មី "តេជោ"**
....	....

ឧបសម្ព័ន្ធ៣៖ ពាក្យស្នើសុំបោះបង់សមាជិកភាពពីថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា

ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ពាក្យស្នើសុំបោះបង់សមាជិកភាពពីថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា (ថ.ផ.ទ.)

សូមគោរពជូន
ឯកឧត្តមនាយក មជ្ឈមណ្ឌលបណ្តុះធុរកិច្ចថ្មី "តេជោ"

កម្មវត្ថុ ៖ សំណើសុំបោះបង់សមាជិកភាពពីថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា។

មូលហេតុ៖ ....
....។

សេចក្តីដូចមានចែងក្នុងកម្មវត្ថុ និងមូលហេតុខាងលើ ខ្ញុំសូមគោរពជម្រាបជូន **ឯកឧត្តមនាយក** មេត្តាអនុញ្ញាតឱ្យ៖ ឈ្មោះអង្គភាពស្នើសុំ:...ជាអក្សរឡាតាំង:..............................
ប្រភេទអង្គភាព/ក្រុមហ៊ុន:...តំណាងដោយ (ឈ្មោះអ្នកតំណាងស្របច្បាប់របស់អង្គភាព/ក្រុមហ៊ុន):......................................□អត្តសញ្ញាណប័ណ្ណ/□លិខិតឆ្លងដែនលេខ:...........................
លេខទូរស័ព្ទ:..អ៊ីម៉ែល:..អាសយដ្ឋានបច្ចុប្បន្ន:
....
អាចបោះបង់សមាជិកភាពពីថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា។

អង្គភាពស្នើសុំ យល់ព្រមទទួលយក នូវគ្រប់លក្ខខណ្ឌដូចមានចែងក្នុង "នីតិវិធីនៃការបញ្ចប់សមាជិកភាព", ចូលរួមសហការជម្រះប្រតិបត្តិការផ្លាស់ប្តូរទិន្នន័យ ដែលនៅសេសសល់, ដោះស្រាយបញ្ហាបច្ចេកទេសពាក់ព័ន្ធតាមការចាំបាច់ និងដោះស្រាយបញ្ហា ឬវិវាទនានា ដើម្បីធានាថាការស្នើសុំបោះបង់សមាជិកភាព មិនប៉ះពាល់ដល់សមាជិកដទៃ និងដំណើរការរបស់ **ថ.ផ.ទ.**។

សូមគោរពភ្ជាប់មកជាមួយនូវ៖

- លិខិតផ្ទេរសិទ្ធិ (ក្នុងករណី អ្នកតំណាងមិនមែននាយកប្រតិបត្តិ ឬប្រធានស្ថាប័ន)

ខ្ញុំសូមធានាអះអាង៖

- រាល់ព័ត៌មានទាំងអស់ដែលបានបំពេញនៅក្នុងពាក្យស្នើសុំនេះ ពិត និង ត្រឹមត្រូវ
- ពាក្យស្នើសុំត្រូវបានធ្វើឡើងក្នុងដែនសមត្ថកិច្ចរបស់អង្គភាពស្នើសុំ
- បានផ្តល់ឯកសារពាក់ព័ន្ធ និងគោរពតាមរាល់លក្ខខណ្ឌដូចមានកំណត់ក្នុង "នីតិវិធីនៃការបញ្ចប់សមាជិកភាព" ។

អាស្រ័យដូចបានគោរពជម្រាបជូនខាងលើ, សូម **ឯកឧត្តមនាយក** មេត្តាអនុញ្ញាតតាមការស្នើសុំដោយក្តីអនុគ្រោះ។

ថ្ងៃ..........................ខែ...........ឆ្នាំ..........ព.ស.............
រាជធានីភ្នំពេញ ថ្ងៃទី........ ខែ.............ឆ្នាំ.............
នាយកប្រតិបត្តិ/ប្រធានស្ថាប័ន/អ្នកតំណាងស្របច្បាប់

ឧបសម្ព័ន្ធ៤៖ នីតិវិធីបញ្ចប់សមាជិកភាព

នីតិវិធីបញ្ចប់សមាជិកភាព

១. នីតិវិធីនៃការបញ្ចប់សមាជិកភាព អនុវត្តចំពោះតែសមាជិកដោយការស្នើសុំ ដែលមានបំណងបោះបង់សមាជិកភាព ឬត្រូវបានបញ្ចប់សមាជិកភាពតាមសេចក្តីសម្រេច របស់ប្រតិបត្តិករ **ថ.ផ.ទ.**។

២. នៅពេលសមាជិកដោយការស្នើសុំ បោះបង់សមាជិកភាពតាមការដាក់ពាក្យស្នើសុំ ឬប្រតិបត្តិករ **ថ.ផ.ទ.** បានសម្រេចបញ្ចប់សមាជិកភាពរបស់សមាជិកពី **ថ.ផ.ទ.** ដោយមានការជូនដំណឹងជាមុន, សមាជិកដោយការស្នើសុំនោះ ត្រូវផ្សព្វផ្សាយជាសាធារណៈដល់សមាជិកដទៃទៀត និងភាគីពាក់ព័ន្ធ ដើម្បីជម្រះ ឬទូទាត់រាល់ប្រតិបត្តិការដែលមិនទាន់បានបញ្ចប់, ដោះស្រាយបញ្ហាបច្ចេកទេសពាក់ព័ន្ធតាមការចាំបាច់, ឬដោះស្រាយវិវាទនានា ដើម្បីធានាថាការស្នើសុំបោះបង់សមាជិកភាព មិនប៉ះពាល់ដល់សមាជិកដទៃ និងដំណើរការរបស់ **ថ.ផ.ទ.** តាមកាលកំណត់របស់ប្រតិបត្តិករ **ថ.ផ.ទ.**។

៣. ក្នុងករណីសមាជិកដោយការស្នើសុំ មិនអាចបំពេញកាតព្វកិច្ច ដូចបានបញ្ជាក់ក្នុងចំណុចទី២ខាងលើ បានទាន់ពេលវេលាតាមកាលកំណត់ ឬក្នុងករណីប្រតិបត្តិករ **ថ.ផ.ទ.** សម្រេចបញ្ចប់សមាជិកភាពជាបន្ទាន់ ដោយមិនបានជូនដំណឹងជាមុន តាមឆន្ទានុសិទ្ធិរបស់ខ្លួន, ភាគីពាក់ព័ន្ធត្រូវដោះស្រាយវិវាទដោយសន្តិវិធី តាមរយៈការចរចា ឬការសម្រុះសម្រួលឱ្យអស់លទ្ធភាពជាមុនសិន មុននឹងឈានដល់ការប្តឹងទៅស្ថាប័នមានសមត្ថកិច្ច ដើម្បីដោះស្រាយតាមច្បាប់នៃព្រះរាជាណាចក្រកម្ពុជា។

៤. សមាជិកដោយការស្នើសុំ ត្រូវទទួលខុសត្រូវរាល់បន្ទុកចំណាយទាំងអស់ ពាក់ព័ន្ធនឹងការបោះបង់សមាជិកភាព ឬការបញ្ចប់សមាជិកភាពតាមសេចក្តីសម្រេចរបស់ប្រតិបត្តិករ **ថ.ផ.ទ.**។

៥. ការបញ្ចប់សមាជិកភាពពី **ថ.ផ.ទ.** ត្រូវមានប្រសិទ្ធភាព គិតចាប់ពីថ្ងៃទទួលបានសេចក្តីជូនដំណឹងស្តីពីការបញ្ចប់សមាជិកភាពជាស្ថាពរ ដែលចេញដោយប្រតិបត្តិករ **ថ.ផ.ទ.** ។

ឧបសម្ព័ន្ធ៥៖ ឯកសារណែនាំក្នុងការដំឡើងម៉ាស៊ីនសុវត្ថិភាព (Security Server Installation Guideline)

ឧបសម្ព័ន្ធ៦៖ ឯកសារធានានូវគុណភាព និងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (Information Security Guideline)

ឧបសម្ព័ន្ធ៧៖ បញ្ជីត្រួតពិនិត្យគុណភាព និងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (Information Security Checklist)

ឧបសម្ព័ន្ធ៨៖ CamDigiKey KYC Verification API

ឧបសម្ព័ន្ធ៥៖ ឯកសារណែនាំក្នុងការដំឡើងម៉ាស៊ីនសុវត្ថិភាព (Security Server Installation Guideline)

STANDALONE SECURITY SERVER INSTALLATION AND CONFIGURATION

By CamDX Operator

July 2022

DOCUMENT VERSION HISTORY

RELEASE NO	AUTHOR	DATE	BRIEF SUMMARY OF CHANGES
V1.0.0	CamDX Operator	JULY/2022	

Contents

TABLES

Figures

1. SECURITY SERVER REQUIREMENT

1.1 Hardware: (Minimum Recommended)

- CPU: 64-bit dual-core Intel
- RAM: 4GB
- Network Card: 100 Mbps

1.2 Software:

- Operating System: Ubuntu 18.04 LTS x86-64
  - Add System User
    - **sudo adduser camdx-systemadmin**
- Set the operating system locale.
  - Add following line to the **/etc/environment.**
    - **LC_ALL=en_US.UTF-8**
- Ensure that the packages locales and software-properties-common are present
  - **sudo apt-get install locales software-properties-common**
- Ensure that the timezone is set to Asia/Phnom_Penh – timedatectl
  - **sudo timedatectl set-timezone Asia/Phnom_Penh**

1.3 Network Ports

It is strongly recommended to protect the security server from unwanted access using a firewall (hardware or software based). The firewall can be applied to both incoming and outgoing connections depending on the security requirements of the environment where the security server is deployed. It is recommended to allow incoming traffic to specific ports only from explicitly defined sources using IP filtering. Special attention should be paid with the firewall configuration since incorrect configuration may leave the security server vulnerable to exploits and attacks.

The table below lists the required connections between different components.

Connection Type	Source	Target	Target Ports	Protocol	Note
Out	Security Server	Central Server	80, 4001	tcp	
Out	Security Server	Management Security Server	5500, 5577	tcp	
Out	Security Server	OCSP Service	80 / 443	tcp	
Out	Security Server	Timestamping Service	80 / 443	tcp	
Out	Security Server	Data Exchange Partner Security Server (Service Producer)	5500, 5577	tcp	
Out	Security Server	Producer Information System	80, 443, other	tcp	Target in the internal network

Connection Type	Source	Target	Target Ports	Protocol	Note
In	Monitoring Security Server	Security Server	5500, 5577	tcp	
In	Data Exchange Partner Security Server (Service Consumer)	Security Server	5500, 5577	tcp	
In	Consumer Information System	Security Server	80, 443	tcp	Source in the internal network
In	Admin	Security Server	4000	tcp	Source in the internal network

TABLE 1 – NETWORK PORTS

1.4 Network Diagram

The network diagram below provides an example of a basic Security Server setup. Allowing incoming connections from the Monitoring Security Server on ports 5500/tcp and 5577/tcp is necessary for the CamDX Operator to be able to monitor the ecosystem and provide statistics and support for Members.

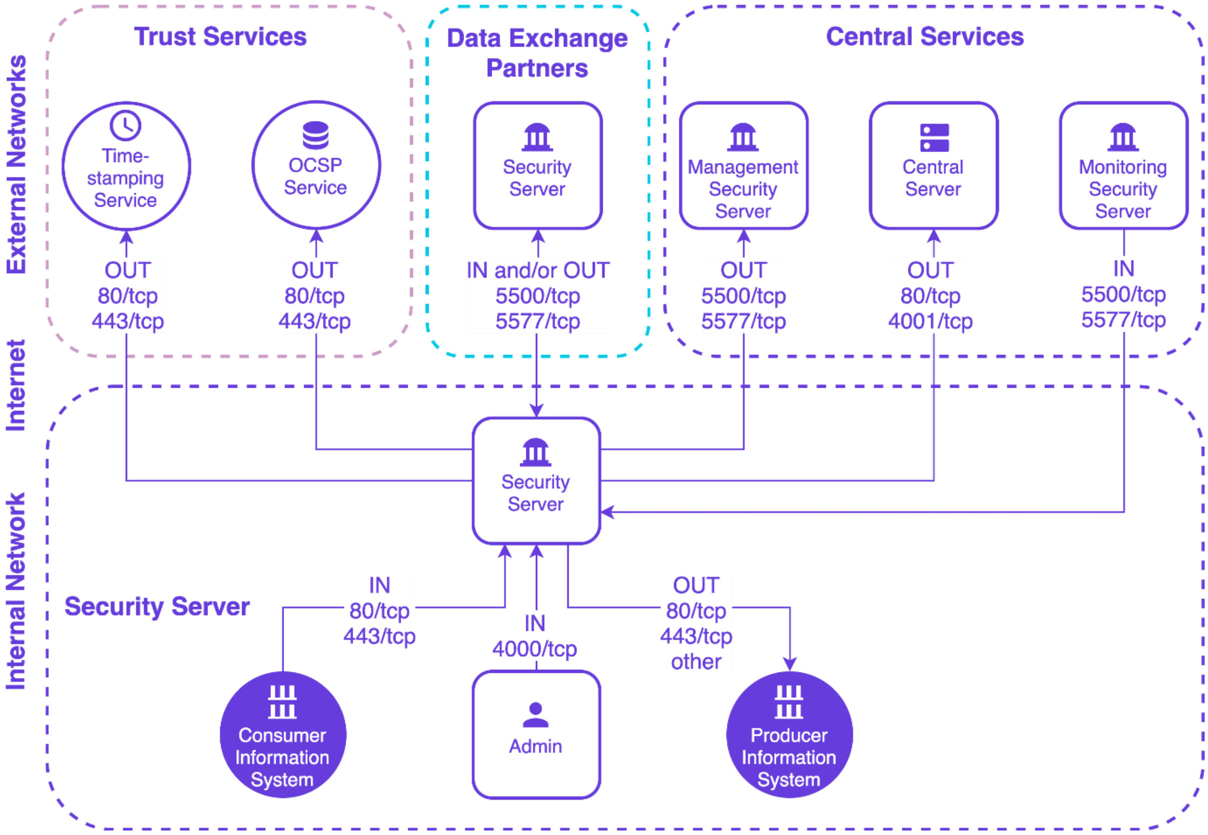


FIGURE 1 – NETWORK DIAGRAM

1.5 CamDX Central Authority IP's for Whitelisting

Type	CamDX - Production	CamDX - Dev
Central Server	103.63.190.230 103.63.190.232	206.189.151.1
Central Monitoring Server	103.63.190.227	
Management Security Server	103.63.190.231 103.63.190.233	178.128.122.111

2. INSTALLATION

2.1 CamDX Security Server Built Packages

- Add Repository to **/etc/apt/sources.list**:
    - **deb [arch=all,amd64] http://repository.camdx.gov.kh/repository/camdx-release bionic main**
- Add Signing Key:
    - **curl http://repository.camdx.gov.kh/repository/camdx-anchors/api/gpg/key/0x04194DBF-pub.asc | sudo apt-key add –**

2.2 Remote Database (Optional)

if you want to use remote database server instead of the default locally installed one, you need to pre-create configuration file containing the database administrator master password. This can be done by performing the following steps:

- sudo touch /etc/xroad.properties
- sudo chown root:root /etc/xroad.properties
- sudo chmod 600 /etc/xroad.properties

Edit **/etc/xroad.properties** contents.

- postgres.connection.password = 54F46A19E50C11DA8631468CF09BE5DB

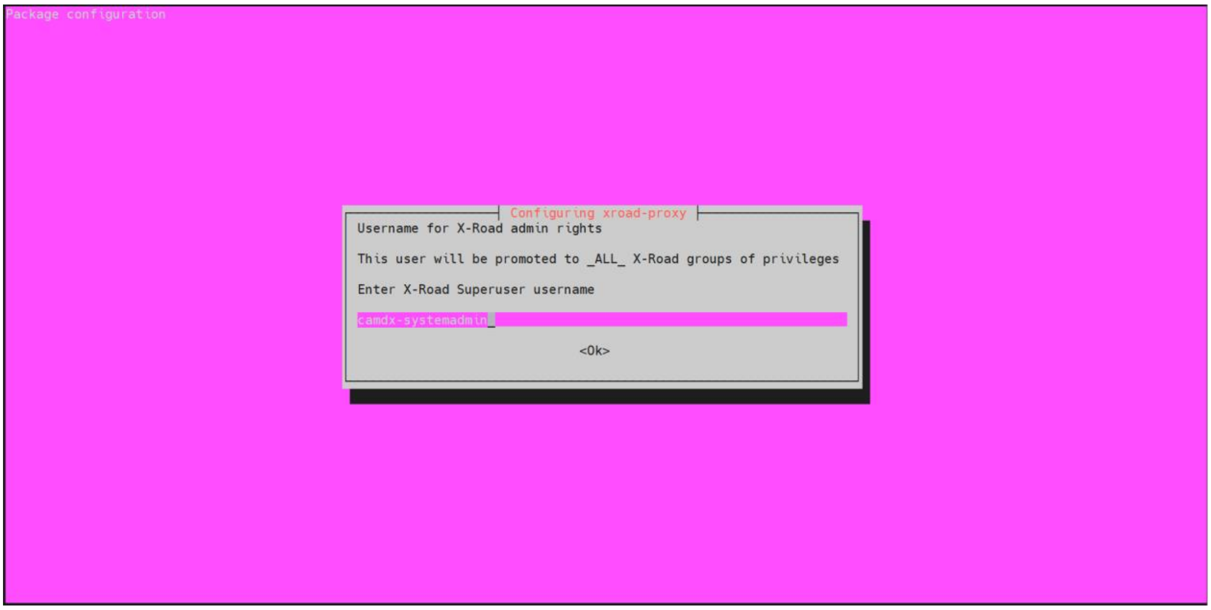
2.3 Install the CamDX Package

- **sudo apt-get update**
- **sudo apt-get install xroad-securityserver**

Upon the first installation of the packages, the system asks for the following information.

- Account name for the user who will be granted the rights to perform all activities in the user interface
- Database server URL. Locally installed database is suggested as default but remote databases can be used as well. In case remote database is used, one should verify that the version of the local PostgreSQL client matches the version of the remote PostgreSQL Server.
- The Distinguished Name of the owner of the user interface's and management REST API's self-signed TLS certificate(Subject DN) and its alternative names (subjectAltName)

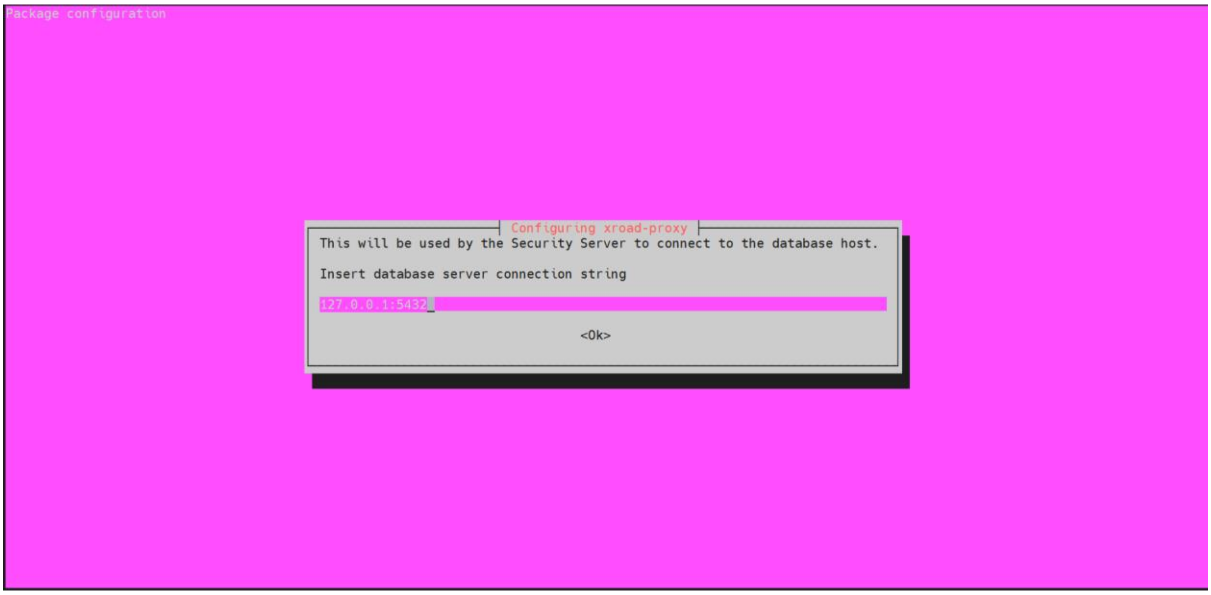
Account name for the user who will be granted the rights to perform all activities in the user interface



```
Package configuration

┤ Configuring xroad-proxy ├
Username for X-Road admin rights

This user will be promoted to _ALL_ X-Road groups of privileges

Enter X-Road Superuser username

camdx-systemadmin_

<Ok>
```

FIGURE 2 – SPECIFY SUPERADMIN USER

Database server URL. Locally installed database is suggested as default, but remote databases can be used as well.

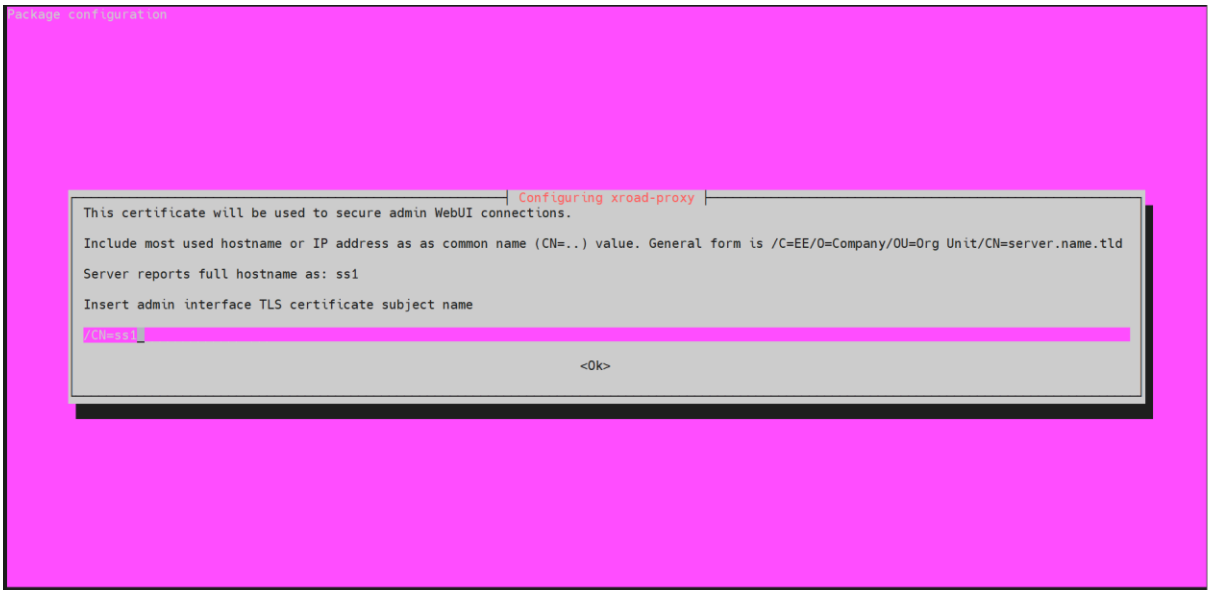


```
Package configuration

┤ Configuring xroad-proxy ├
This will be used by the Security Server to connect to the database host.

Insert database server connection string

127.0.0.1:5432_

<Ok>
```

FIGURE 3 – LOCAL DATABASE CONNECTION STRING

The Distinguished Name of the owner of the user interface's and management REST API's self-signed TLS certificate(Subject DN) and its alternative names

E.g: /C=KH/O=EXAMPLE MINISTRY or COMPANY/OU=ICT Department/CN=HOSTNAME or FQDN or IP

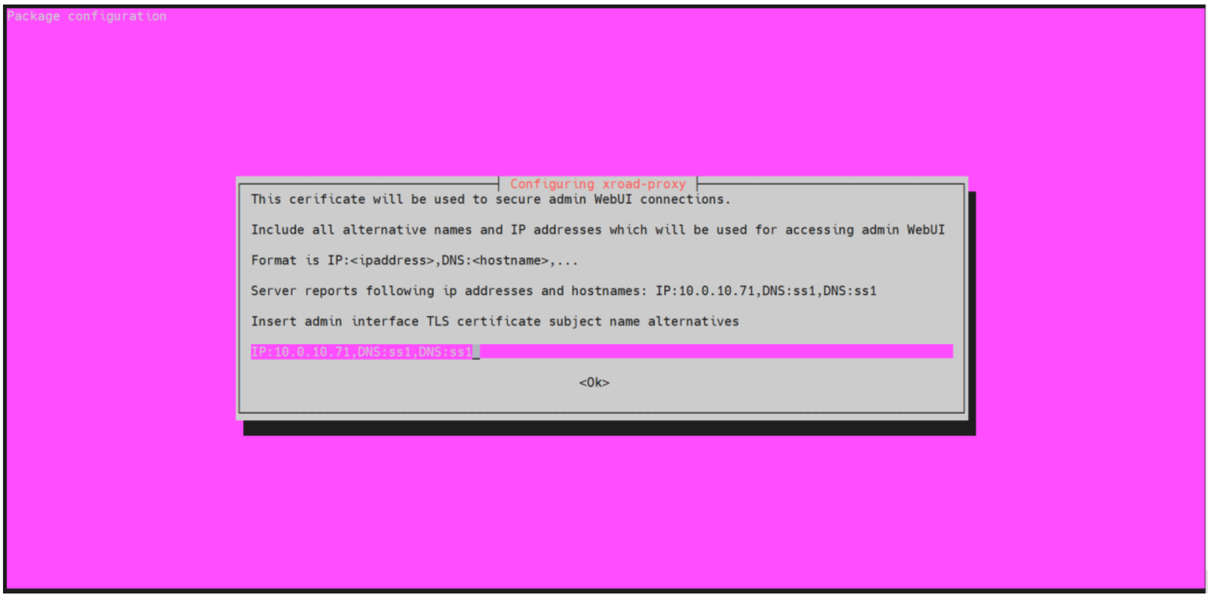


```
Package configuration

                              ┤ Configuring xroad-proxy ├
 This certificate will be used to secure admin WebUI connections.

 Include most used hostname or IP address as as common name (CN=..) value. General form is /C=EE/O=Company/OU=Org Unit/CN=server.name.tld

 Server reports full hostname as: ss1

 Insert admin interface TLS certificate subject name

 /CN=ss1_

                                   <Ok>
```

FIGURE 4 – TLS CERTIFICATE

The Distinguished Name of the owner of the user interface's and management REST API's self-signed TLS certificate(Subject DN) and its alternative names

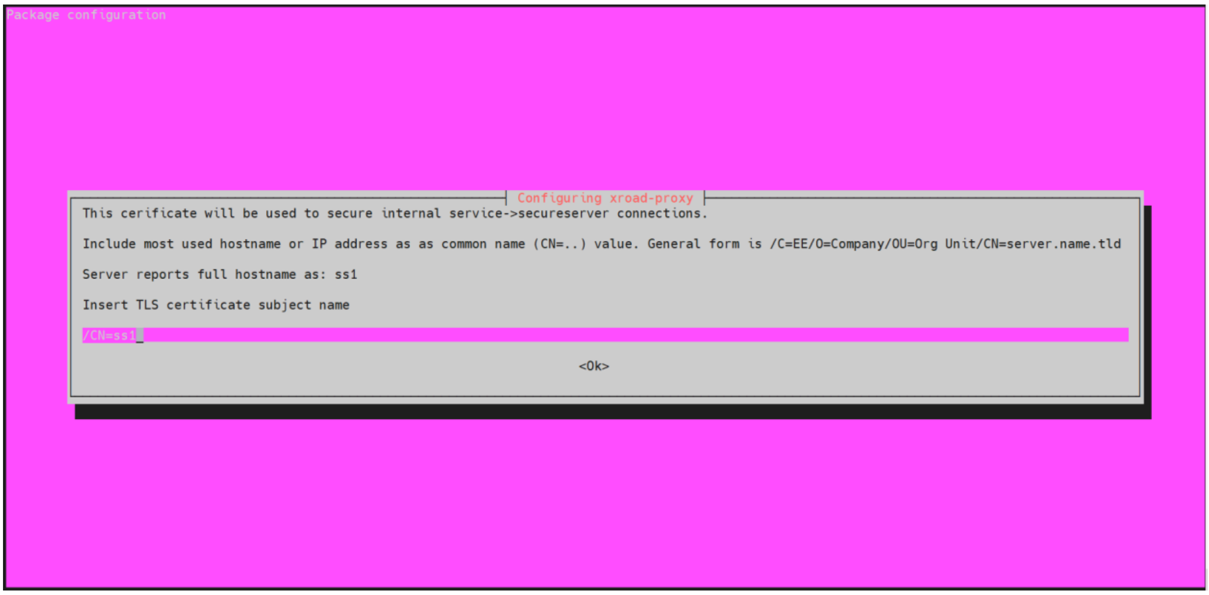
E.g: /C=KH/O=EXAMPLE MINISTRY or COMPANY/OU=ICT Department/CN=HOSTNAME or FQDN or IP



```
Package configuration

                       ┤ Configuring xroad-proxy ├
 This cerificate will be used to secure admin WebUI connections.

 Include all alternative names and IP addresses which will be used for accessing admin WebUI

 Format is IP:<ipaddress>,DNS:<hostname>,...

 Server reports following ip addresses and hostnames: IP:10.0.10.71,DNS:ss1,DNS:ss1

 Insert admin interface TLS certificate subject name alternatives

 IP:10.0.10.71,DNS:ss1,DNS:ss1_

                               <Ok>
```

FIGURE 5 – TLS CERTIFICATE 2

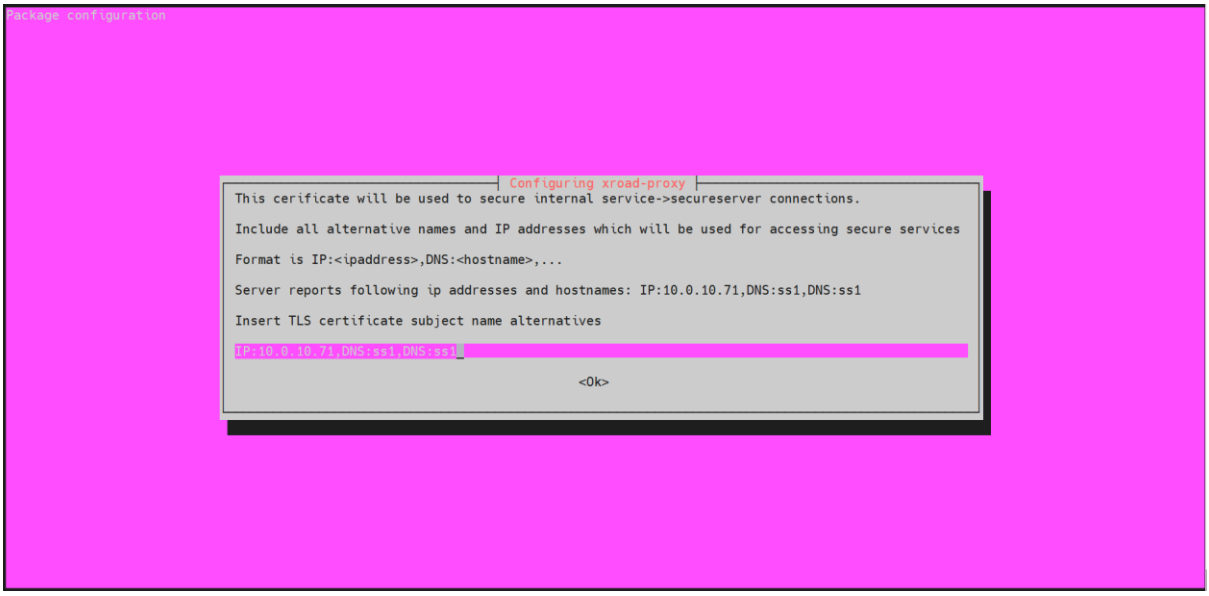
The Distinguished Name of the owner of the TLS certificate that is used for securing the HTTPS access point of information systems. The name and IP addresses detected from the system are suggested as default values.



```
Package configuration

┤ Configuring xroad-proxy ├
This cerificate will be used to secure internal service->secureserver connections.

Include most used hostname or IP address as as common name (CN=..) value. General form is /C=EE/O=Company/OU=Org Unit/CN=server.name.tld

Server reports full hostname as: ss1

Insert TLS certificate subject name

/CN=ss1_

                                   <Ok>
```

FIGURE 6 – INTERNAL SERVICE TLS CERTIFICATE

The Distinguished Name of the owner of the TLS certificate that is used for securing the HTTPS access point of information systems. The name and IP addresses detected from the system are suggested as default values.



```
Package configuration

┤ Configuring xroad-proxy ├
This cerificate will be used to secure internal service->secureserver connections.

Include all alternative names and IP addresses which will be used for accessing secure services

Format is IP:<ipaddress>,DNS:<hostname>,...

Server reports following ip addresses and hostnames: IP:10.0.10.71,DNS:ss1,DNS:ss1

Insert TLS certificate subject name alternatives

IP:10.0.10.71,DNS:ss1,DNS:ss1_

                                   <Ok>
```

FIGURE 7 – INTERNAL SERVICE TLS CERTIFICATE

3. POST-INSTALLATION

3.1 SERVICES CHECK

- sudo systemctl list-units “xroad-*”

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
xroad-confclient.service	loaded	active	running	X-Road confclient
xroad-jetty.service	loaded	active	running	X-Road Jetty server
xroad-monitor.service	loaded	active	running	X-Road Monitor
xroad-proxy.service	loaded	active	running	X-Road Proxy
xroad-signer.service	loaded	active	running	X-Road signer

- Install **xroad-addon-proxymonitor & xroad-addon-opmonitoring**

```
sudo apt install xroad-addon-proxymonitor
sudo apt install xroad-addon-opmonitoring
sudo systemctl restart xroad-opmonitor
```

- Ensure that the security server user interface at https://SECURITYSERVER_IP:4000 can be opened in a Web browser.

4. CONFIGURATION

4.1 SECURITY SERVER MEMBER INFORMATION

- Member Information will be provided by **CamDX Operator**

DEVELOPMENT ENVIRONMENT	
Member Name	Techo Startup Center *
Member Class	GOV
Member Code	DEV00001**

TABLE 2 – MEMBER INFORMATION IN DEVELOPMENT ENVIRONMENT

PRODUCTION ENVIRONMENT	
Member Name	COMPANY1 CO., LTD. *
Member Class	COM
Member Code	PRO00001**

TABLE 3 – MEMBER INFORMATION IN PRODUCTION ENVIRONMENT

- * Member Name in this example are Techo Startup Center and Company1 Co., Ltd.
- ** Member Code will be provided

4.2 ACCESS TO SECURITY SERVER ADMIN INTERFACE

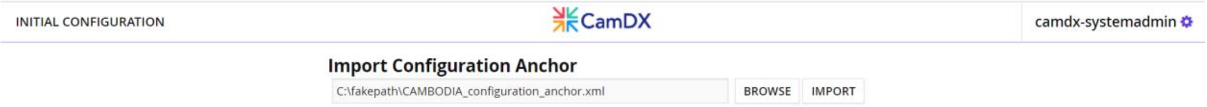
- URL: https://SECURITY_SERVER_IP:4000
- ID: camdx-systemadmin or <YOUR_USERSYSTEMADMIN>
- Password: <YOUR_PASSWORD>

4.3 CONFIGURATION ANCHOR

- The Anchor Configuration file will be provided by CamDX Operator
- You can download it from here:

ENVIRONMENT	
DEV	http://repository.camdx.gov.kh/repository/camdx-anchors/anchors/dev/CAMBODIA_configuration_anchor_dev.xml
PRODUCTION	http://repository.camdx.gov.kh/repository/camdx-anchors/anchors/CAMBODIA_configuration_anchor.xml

- Upload the Configuration Anchor File



Import Configuration Anchor

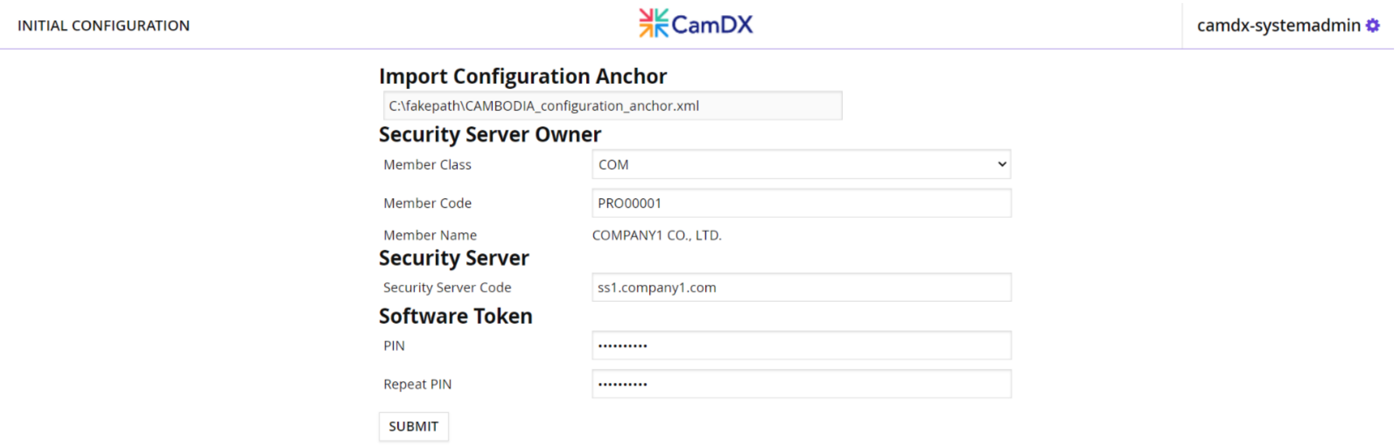
C:\fakepath\CAMBODIA_configuration_anchor.xml

FIGURE 8 – IMPORT CONFIGURATION ANCHOR FILE

4.4 INITIAL CONFIGURATION

With the provided Member Information, fill out the initial configuration page

PRODUCTION ENVIRONMENT	
Member Name	COMPANY1 CO., LTD.
Member Class	COM
Member Code	PRO00001



Import Configuration Anchor

C:\fakepath\CAMBODIA_configuration_anchor.xml

Security Server Owner

Member Class: COM

Member Code: PRO00001

Member Name: COMPANY1 CO., LTD.

Security Server

Security Server Code: ss1.company1.com

Software Token

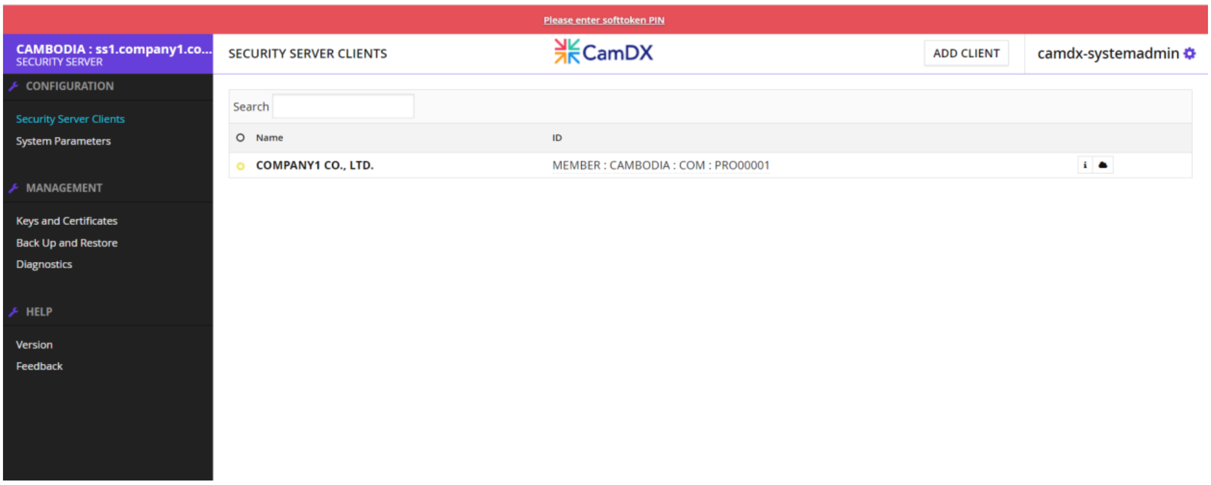
PIN: ••••••••••

Repeat PIN: ••••••••••

FIGURE 9 – INITIAL CONFIGURATION

4.5 ENTERING THE PIN CODE

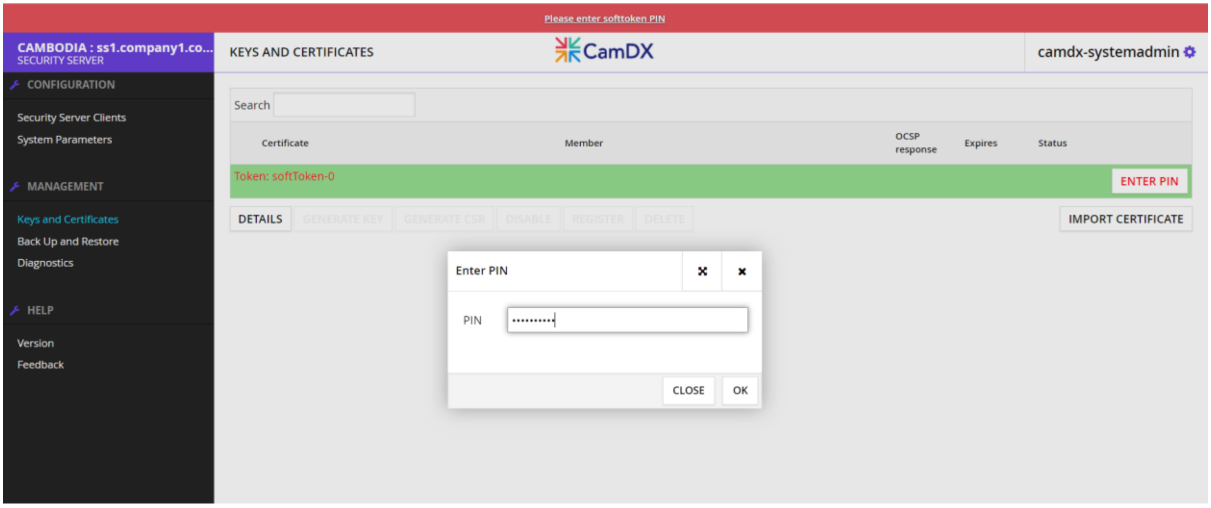
Enter the PIN Code (Software Token) from the Initial Configuration. Click on the “Please enter softtoken PIN” or Navigate through the left panel – Management – Keys and Certificates, to enter the PIN.



Please enter softtoken PIN

Name	ID
COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001

FIGURE 10 – ENTER PIN CODE

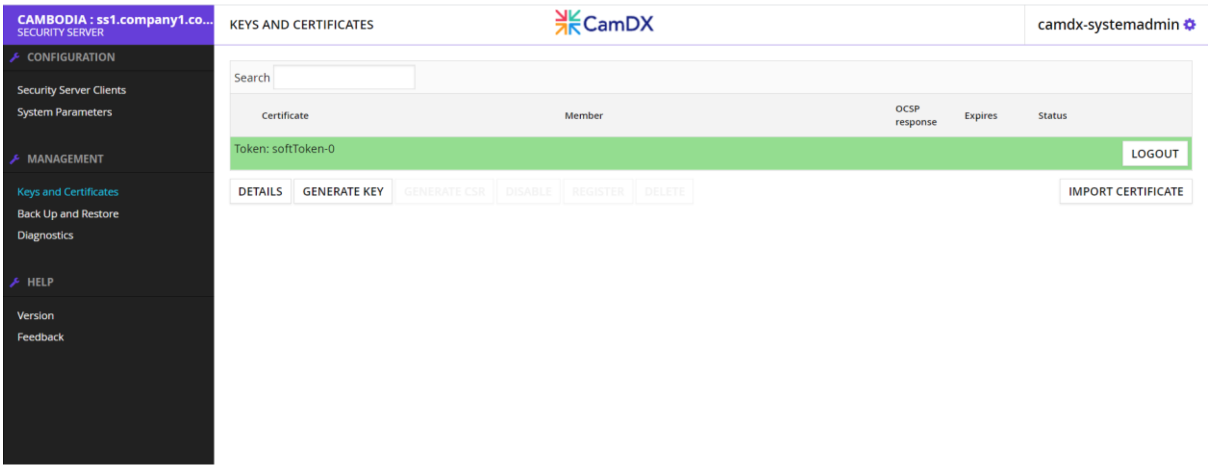


Please enter softtoken PIN

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				

PIN: ••••••••••

FIGURE 11 – ENTER PIN CODE 2

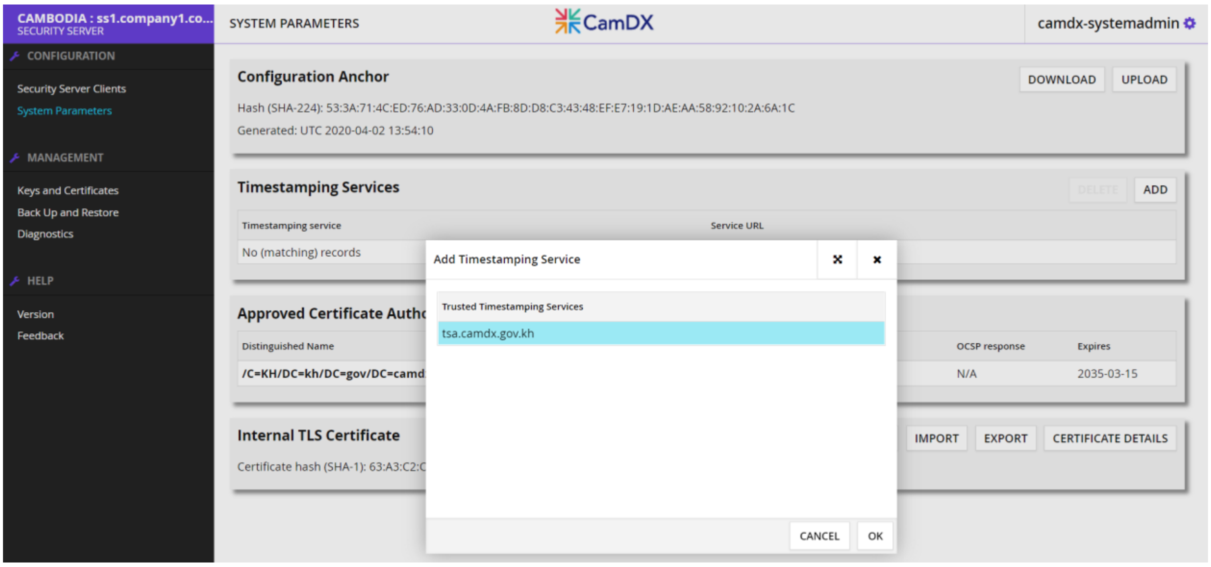


Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				

FIGURE 12 – ENTER PIN CODE 3

4.6 CONFIGURING THE TIME-STAMPING SERVICE

- Choose **System Parameter => Timestamping Services => ADD**
- Pick time-stamping service from the list
- Press **OK**



Configuration Anchor

Hash (SHA-224): 53:3A:71:4C:ED:76:AD:33:0D:4A:FB:8D:D8:C3:43:48:EF:E7:19:1D:AE:AA:58:92:10:2A:6A:1C

Generated: UTC 2020-04-02 13:54:10

Timestamping Services

Timestamping service	Service URL
No (matching) records	

Add Timestamping Service

Trusted Timestamping Services
tsa.camdx.gov.kh

Approved Certificate Autho

Distinguished Name	OCSP response	Expires
/C=KH/DC=kh/DC=gov/DC=camd	N/A	2035-03-15

Internal TLS Certificate

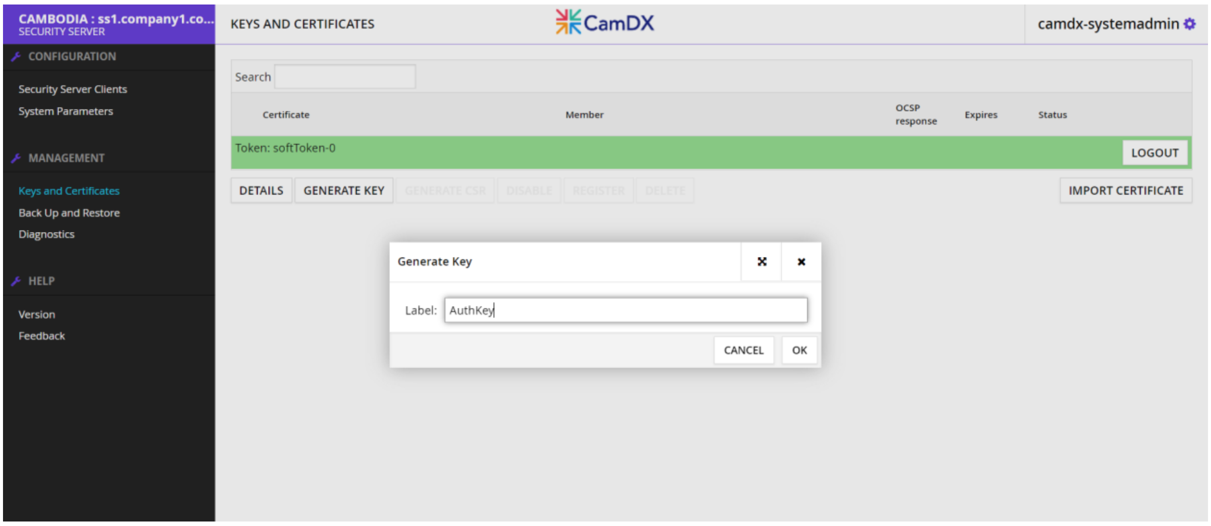
Certificate hash (SHA-1): 63:A3:C2:C

FIGURE 13 – TIMESTAMPING SERVICE

4.7 Sign and Auth Certificates

4.7.1 Auth Certificate

- Generate Auth Certificate Private Key
  - Open **Keys and Certificates**
  - Select Token: **softToken-0**
  - Press **GENERATE KEY**
  - Type Label **AuthKey**
  - Press **OK**
- Generate Auth Certificate Signing Request
  - Select **AuthKey**
  - Press **GENERATE CSR**
  - Choose Usage: **AUTH**
  - Choose Certification Service: **CAMDX INTERMEDIATE CA**
  - CSR Format: **PEM**
  - Press **OK**
  - Specify Organization Name (O): **COMPANY1 CO LTD**
  - Specify Server DNS name (CN): **ss1.company1.com**

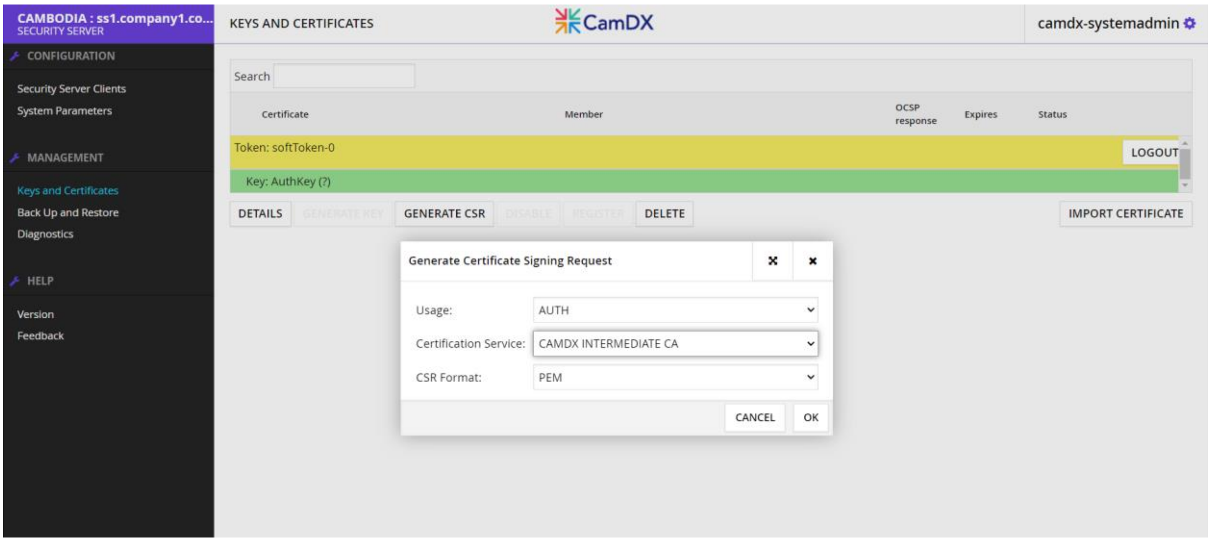


Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				

Generate Key

Label: AuthKey

FIGURE 14 – GENERATING AUTH CERTIFICATE PRIVATE KEY



Token: softToken-0

Key: AuthKey (?)

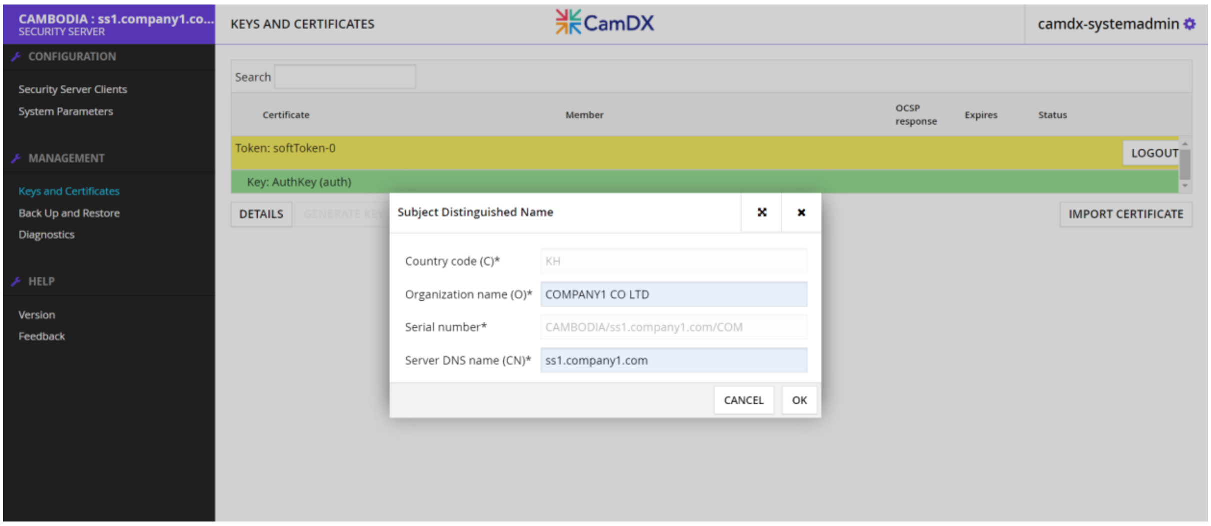
Generate Certificate Signing Request

Usage: AUTH

Certification Service: CAMDX INTERMEDIATE CA

CSR Format: PEM

FIGURE 15 – GENERATING AUTH CERTIFICATE SIGNING REQUEST



Token: softToken-0

Key: AuthKey (auth)

Subject Distinguished Name

Country code (C)* KH

Organization name (O)* COMPANY1 CO LTD

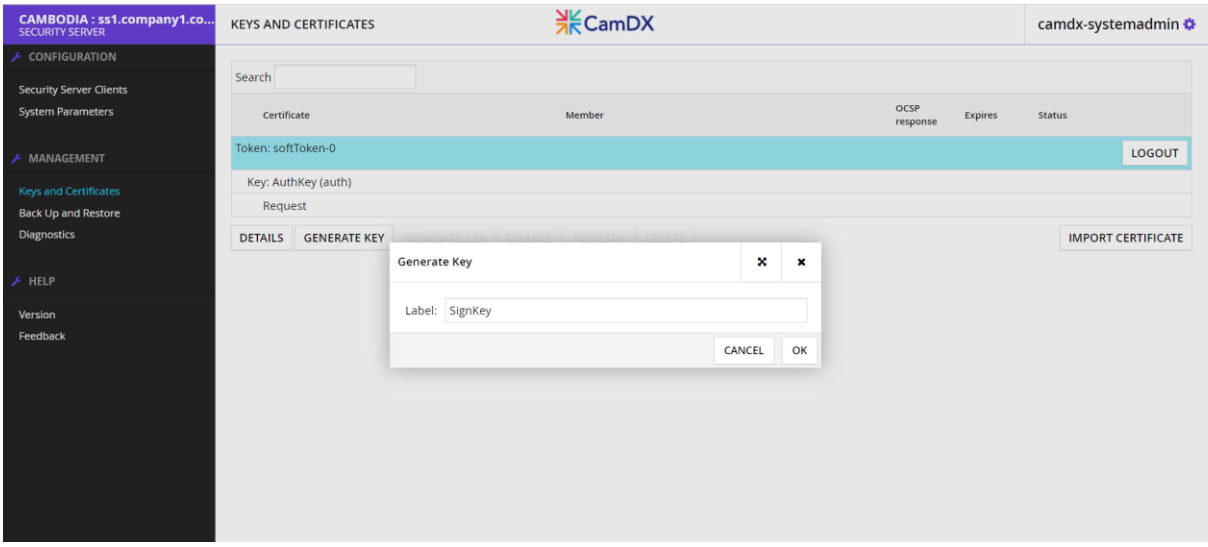
Serial number* CAMBODIA/ss1.company1.com/COM

Server DNS name (CN)* ss1.company1.com

FIGURE 16 – GENERATING AUTH CERTIFICATE SIGNING REQUEST 2

4.7.2 Sign Certificate

- Generate Sign Certificate Signing Request
  - Open **Keys and Certificates**
  - Select Token: softToken-0
  - Press **GENERATE KEY**
  - Type Label **SignKey**
  - Press **OK**
- Generate Auth Certificate Signing Request
  - Select **SignKey**
  - Press **GENERATE CSR**
  - Choose Usage: **SIGN**
  - Choose Certification Service: **CAMDX INTERMEDIATE CA**
  - CSR Format: **PEM**
  - Press **OK**
  - Specify Organization Name (O): **COMPANY1 CO LTD**
  - Specify Server DNS name (CN): **ss1.company1.com**



Token: softToken-0

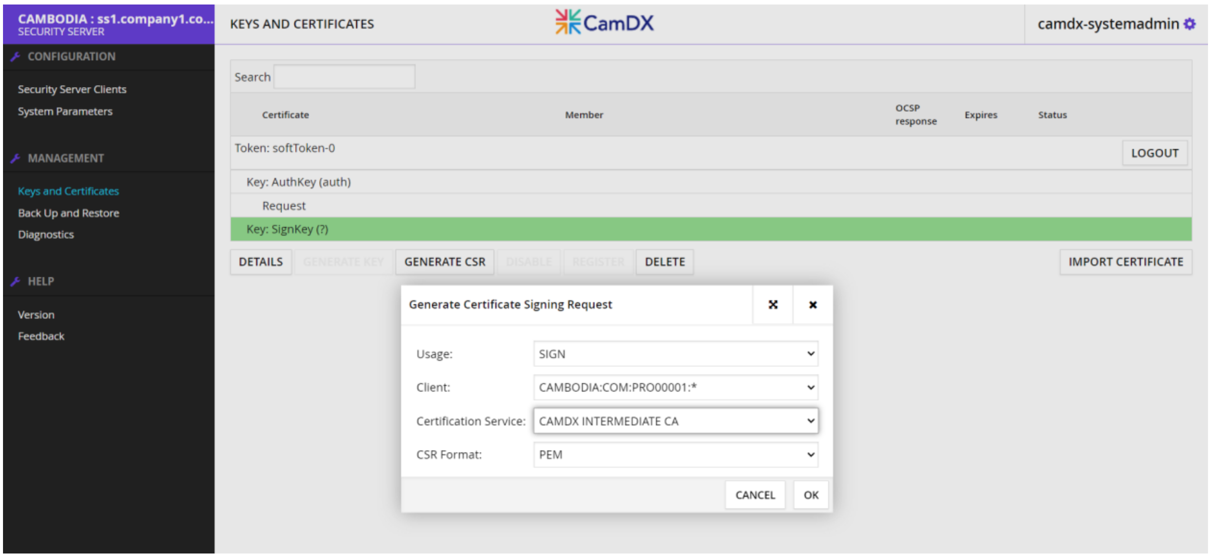
Key: AuthKey (auth)

Request

Generate Key

Label: SignKey

FIGURE 17 – GENERATING SIGN CERTIFICATE PRIVATE KEY



Token: softToken-0

Key: AuthKey (auth)

Request

Key: SignKey (?)

Generate Certificate Signing Request

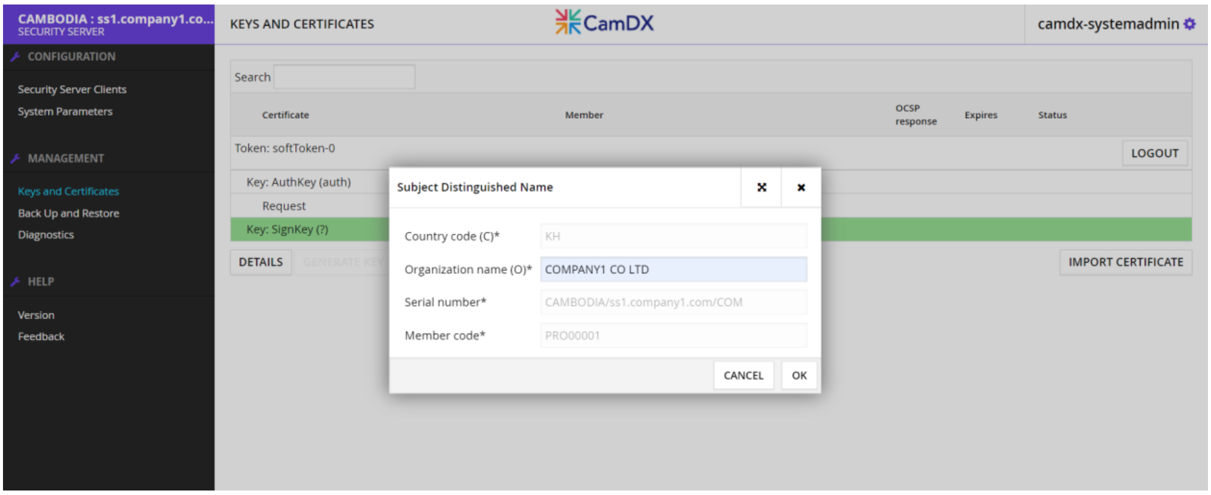
Usage: SIGN

Client: CAMBODIA:COM:PRO00001:*

Certification Service: CAMDX INTERMEDIATE CA

CSR Format: PEM

FIGURE 18 – GENERATING SIGN CERTIFICATE SIGNING REQUEST



Token: softToken-0

Key: AuthKey (auth)

Request

Key: SignKey (?)

Subject Distinguished Name

Country code (C)* KH

Organization name (O)* COMPANY1 CO LTD

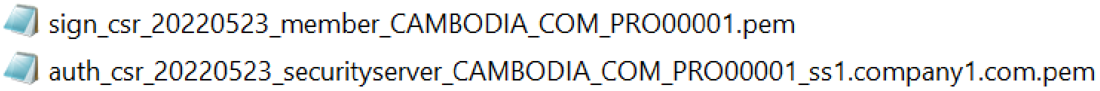
Serial number* CAMBODIA/ss1.company1.com/COM

Member code* PRO00001

FIGURE 19 – GENERATING SIGN CERTIFICATE SIGNING REQUEST 2

4.7.3 Sending the AuthKey and SignKey CSR to CamDX

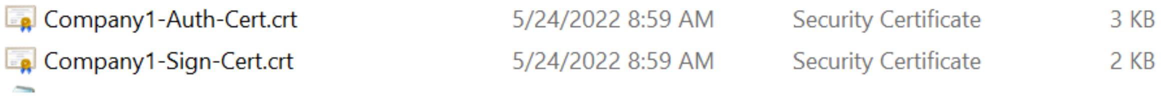
- Contact and Send the CSR Files of "**AuthKey**", and "**SignKey**" to CamDX Central Authority
- Then the CamDX Central Authority will issue the **Auth Certificate** and **Sign Certificate.**



sign_csr_20220523_member_CAMBODIA_COM_PRO00001.pem

auth_csr_20220523_securityserver_CAMBODIA_COM_PRO00001_ss1.company1.com.pem

FIGURE 20 – CERTIFICATE SIGNING REQUESTS

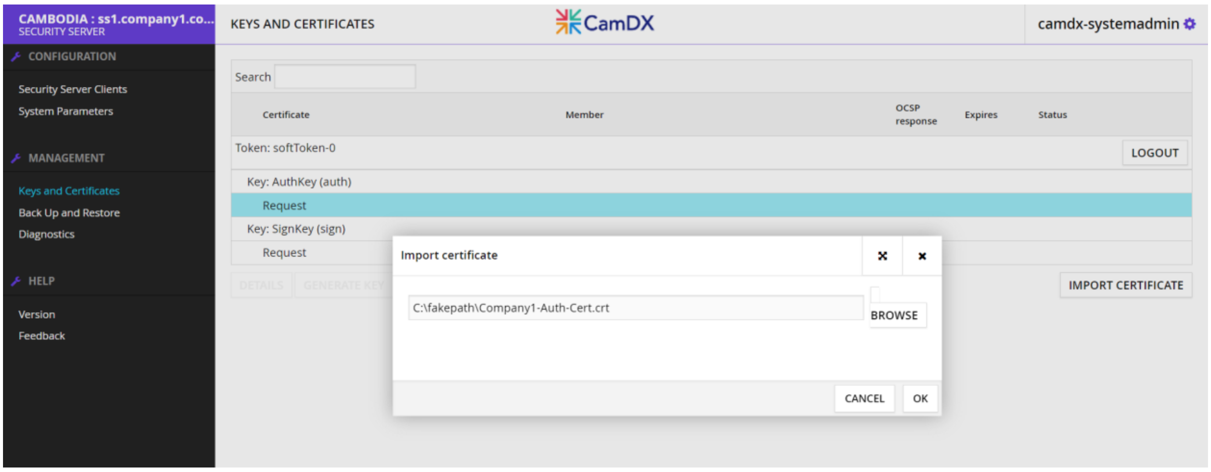


Company1-Auth-Cert.crt	5/24/2022 8:59 AM	Security Certificate	3 KB
Company1-Sign-Cert.crt	5/24/2022 8:59 AM	Security Certificate	2 KB

FIGURE 21 – ISSUED CERTIFICATES RECEIVED

4.8 Importing the certificates

- Select the Certificate request under the **auth key**
  - Press **IMPORT CERTIFICATE**
  - Press **Browse**
  - Press **OK**



Token: softToken-0

Key: AuthKey (auth)

Request

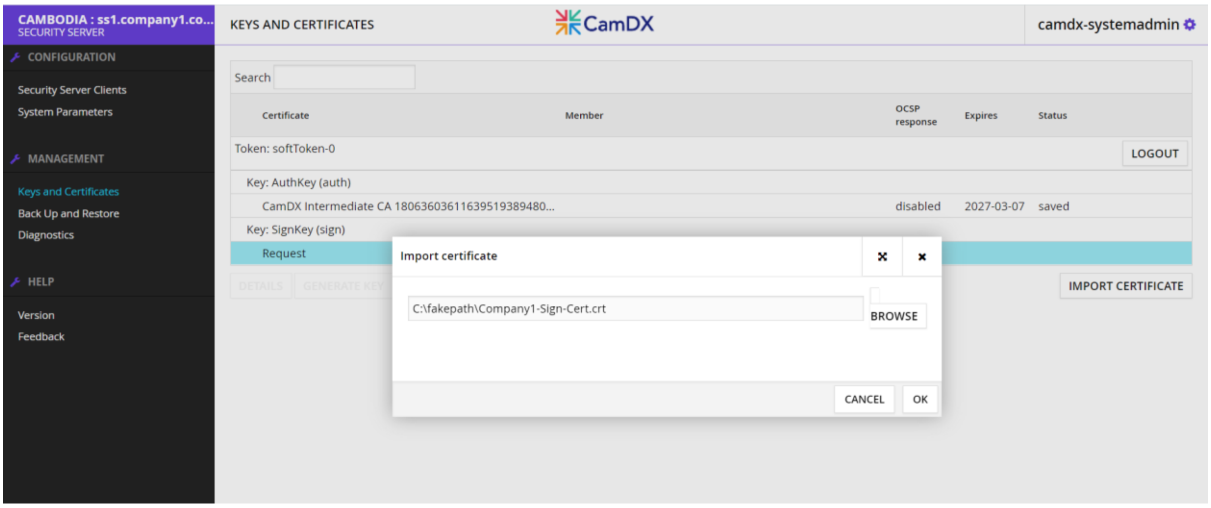
Key: SignKey (sign)

Request

C:\fakepath\Company1-Auth-Cert.crt

FIGURE 22 – IMPORT AUTH CERTIFICATE

- Select the Certificate request under the **sign key**
  - Press **IMPORT CERTIFICATE**
  - Press **Browse**
  - Press **OK**



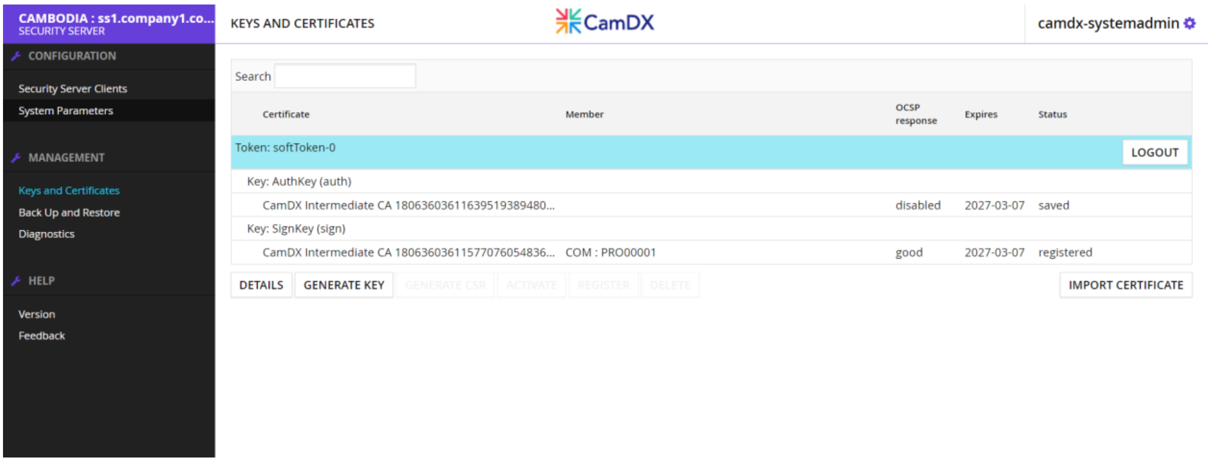
Search

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: AuthKey (auth)				
CamDX Intermediate CA 18063603611639519389480...		disabled	2027-03-07	saved
Key: SignKey (sign)				
Request				

Import certificate

C:\fakepath\Company1-Sign-Cert.crt

FIGURE 23 – IMPORT SIGN CERTIFICATE

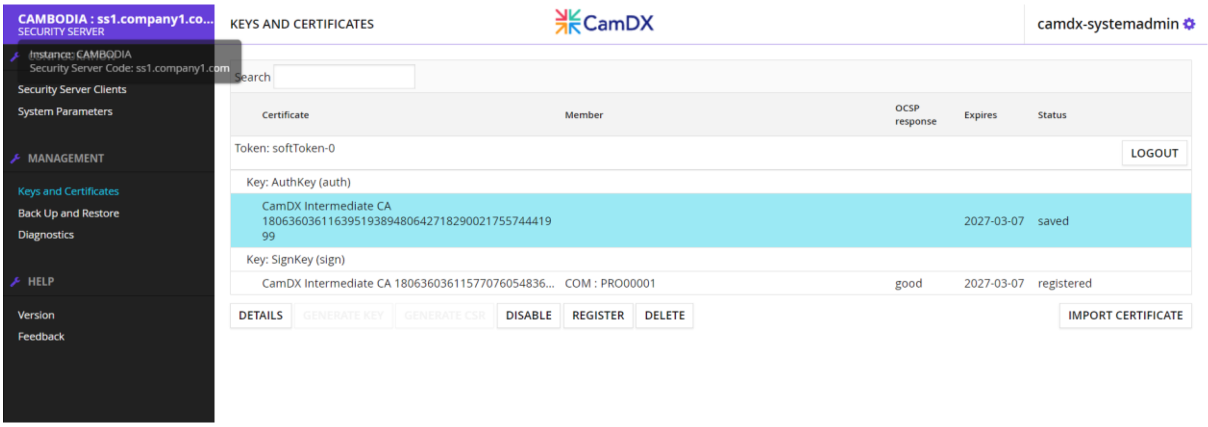


Search

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: AuthKey (auth)				
CamDX Intermediate CA 18063603611639519389480...		disabled	2027-03-07	saved
Key: SignKey (sign)				
CamDX Intermediate CA 18063603611577076054836...	COM : PRO00001	good	2027-03-07	registered

FIGURE 24 – STATUS AFTER BOTH CERTIFICATES IMPORTED

- The Auth Certificate is disabled by default, so we need to activate it:
  - Select the recently imported Auth Certificate
  - Press **ACTIVATE**



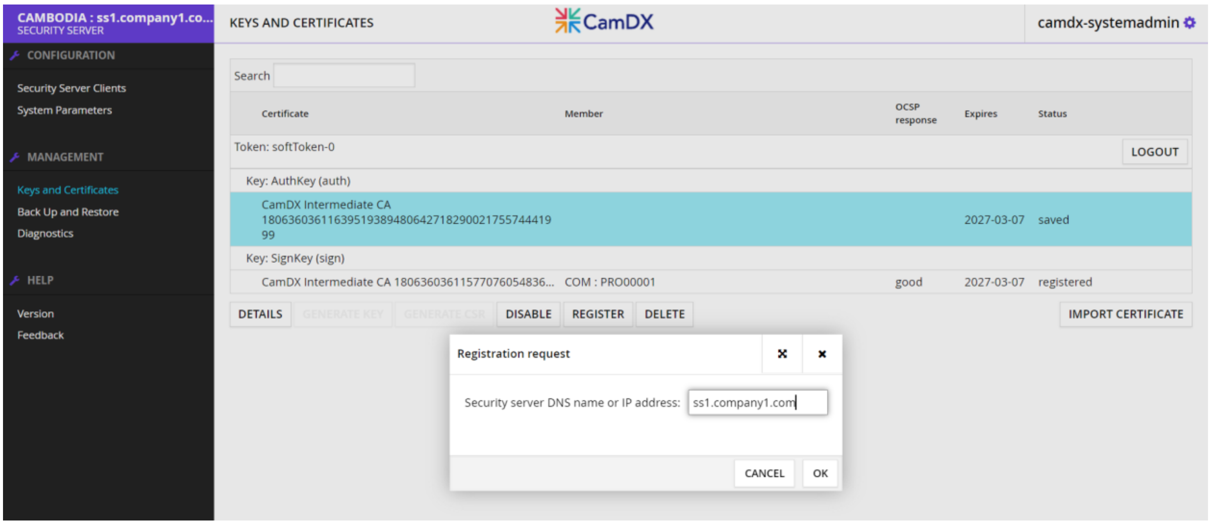
Search

Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: AuthKey (auth)				
CamDX Intermediate CA 18063603611639519389480642718290021755744419 99			2027-03-07	saved
Key: SignKey (sign)				
CamDX Intermediate CA 18063603611577076054836...	COM : PRO00001	good	2027-03-07	registered

FIGURE 25 – ACTIVATE AUTH CERTIFICATE

4.9 REGISTERING THE AUTHENTICATION CERTIFICATE

- Select the **Auth Certificate**
  - Press **REGISTER**
  - Enter **FQDN** (ss1.company1.com)
  - Press **OK** to submit request



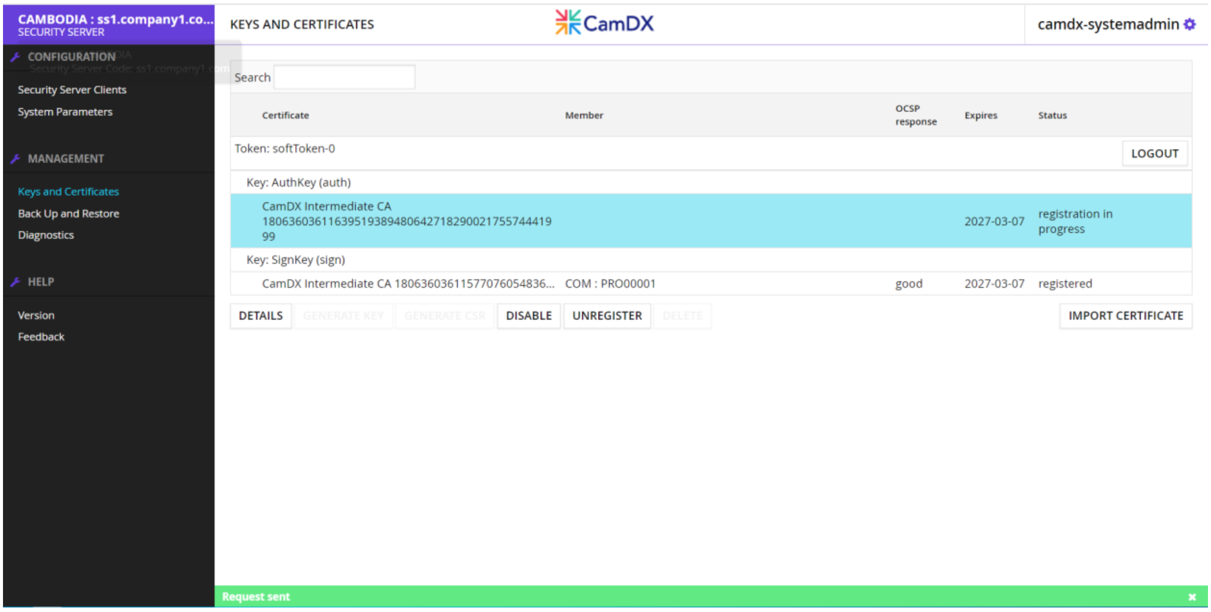
Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: AuthKey (auth)				
CamDX Intermediate CA 180636036116395193894806427182900217557444199			2027-03-07	saved
Key: SignKey (sign)				
CamDX Intermediate CA 1806360361157707605 4836...	COM : PRO00001	good	2027-03-07	registered

Registration request

Security server DNS name or IP address: ss1.company1.com

FIGURE 26 – SEND REGISTRATION REQUEST

- Status after the request showing status “registration in progress”

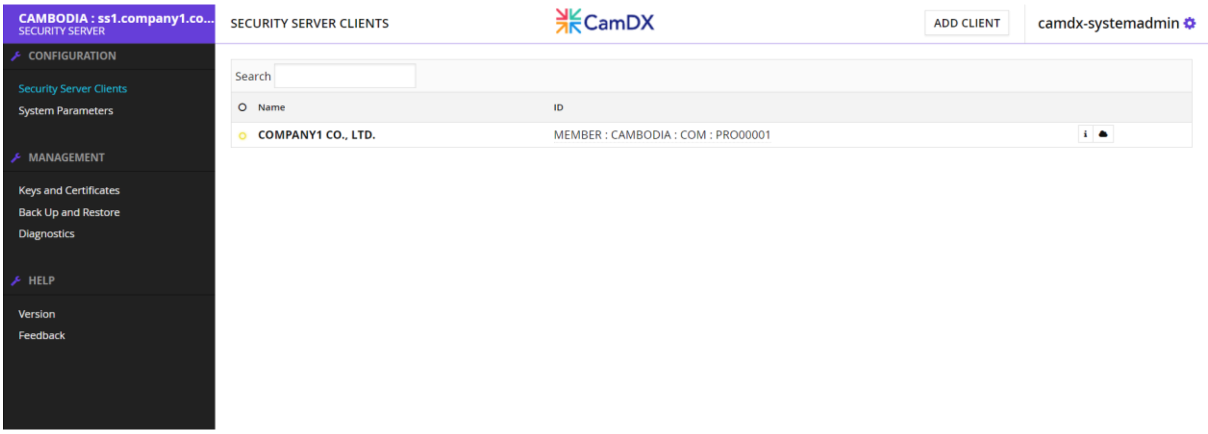


Certificate	Member	OCSP response	Expires	Status
Token: softToken-0				
Key: AuthKey (auth)				
CamDX Intermediate CA 180636036116395193894806427182900217557444199			2027-03-07	registration in progress
Key: SignKey (sign)				
CamDX Intermediate CA 1806360361157707605 4836...	COM : PRO00001	good	2027-03-07	registered

Request sent

FIGURE 27 – STATUS REGISTRATION IN PROGRESS

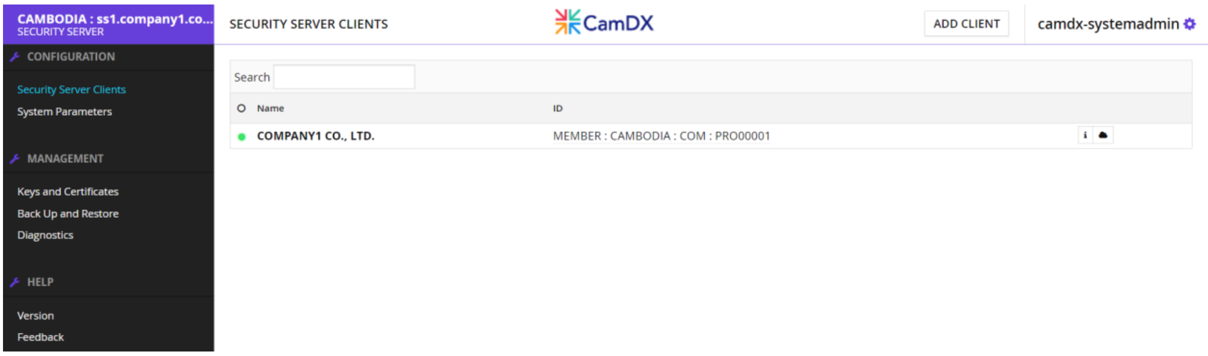
- Status of the Security Server Client is YELLOW while waiting for the approval.



○	Name	ID
○	COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001

FIGURE 28 – STATUS PENDING APPROVAL

- After the CamDX Operator approved the request, the status of the Security Server Client will turn GREEN.



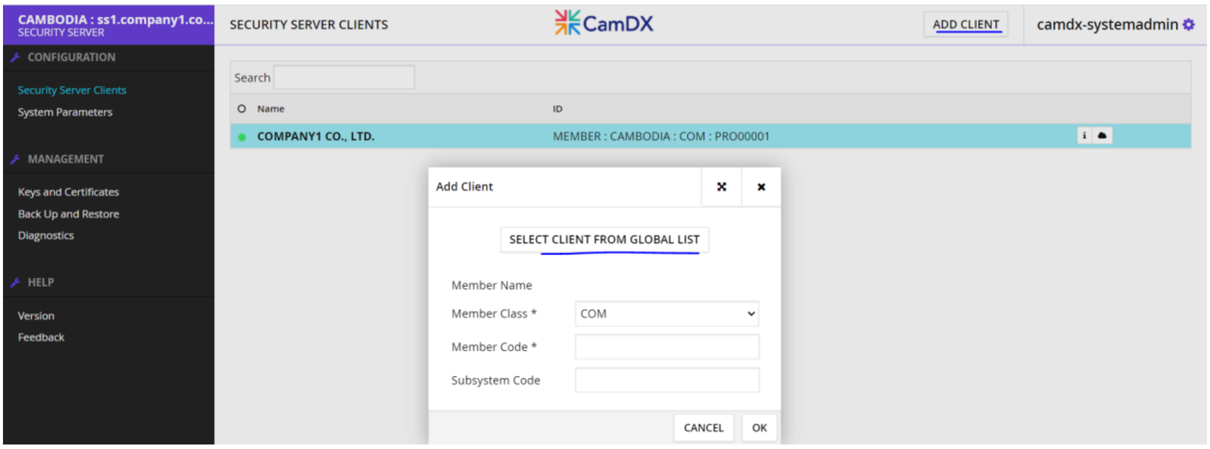
○ Name	ID
● COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001

FIGURE 29 – STATUS AFTER THE APPROVAL

4.10 ADDING A SUBSYSTEM TO SECURITY SERVER

For demonstration purpose, there will be two subsystems added to the security server. A subsystem named “**OPEN_API**” will act as a service provider sharing its API while another subsystem named “**CONSUMER**” will be the one to added to the ACL allowing access to the shared API.

- Open **Security Server Clients**
    - Press **ADD CLIENT**
    - Press **SELECT CLIENT FROM GLOBAL LIST**
    - Press **SEARCH**
    - Select **Member**
    - Press **OK**



○ Name	ID
● COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001

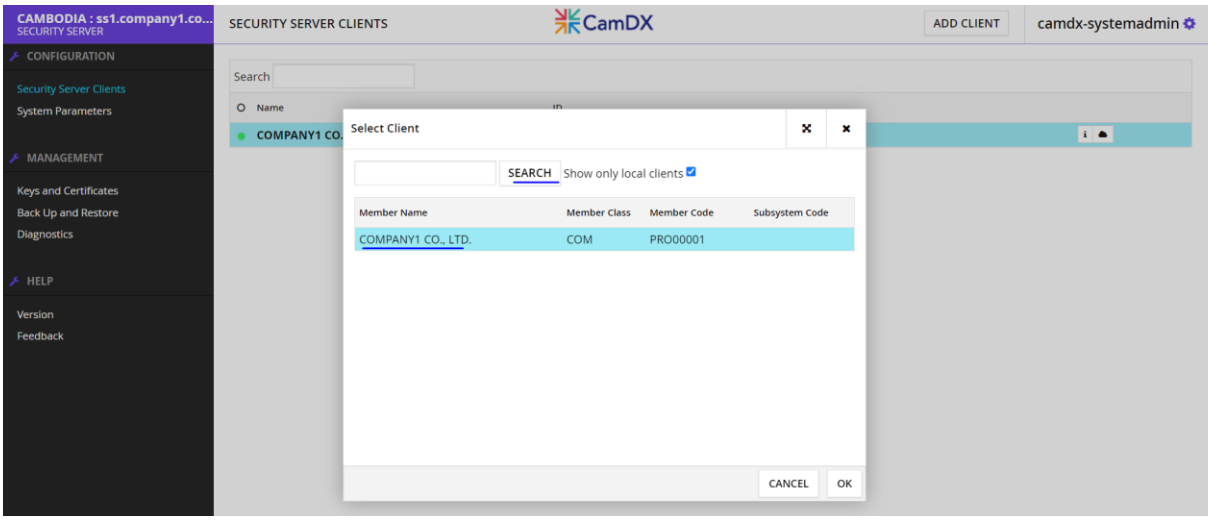
Member Name

Member Class * COM

Member Code *

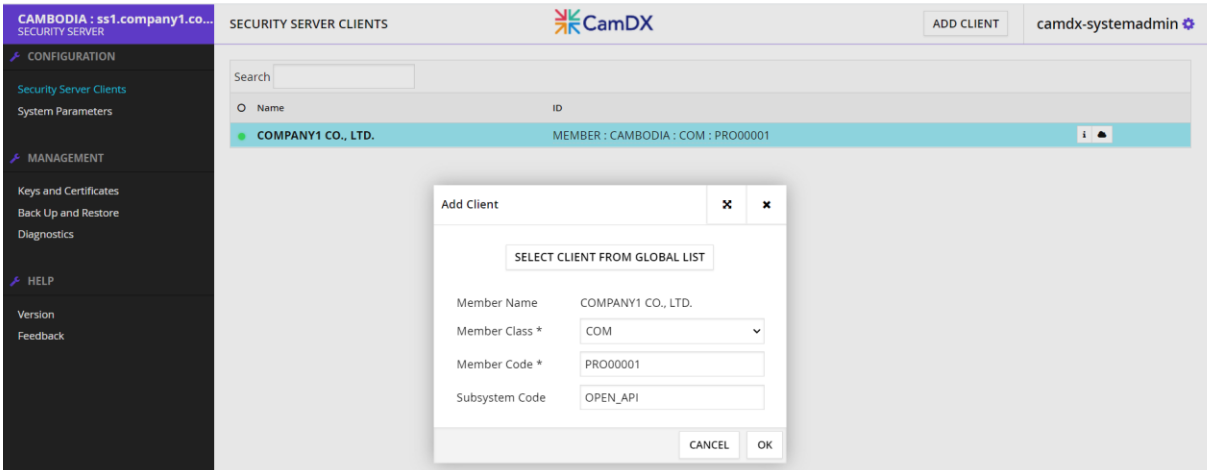
Subsystem Code

FIGURE 30 – ADD A SUBSYSTEM



Member Name	Member Class	Member Code	Subsystem Code
COMPANY1 CO., LTD.	COM	PRO00001	

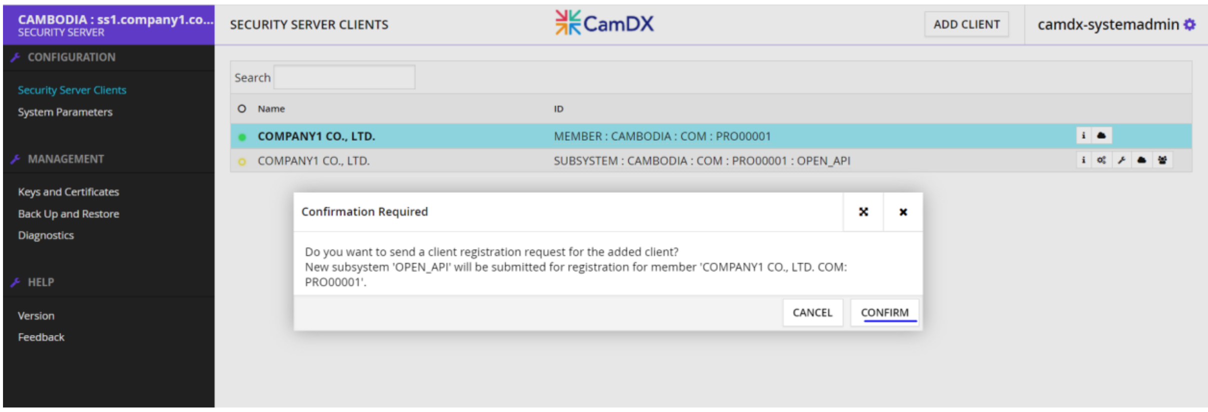
FIGURE 31 – ADD A SUBSYSTEM 2



Name	ID
COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001

Member Name COMPANY1 CO., LTD.
Member Class * COM
Member Code * PRO00001
Subsystem Code OPEN_API

FIGURE 32 – ADD A SUBSYSTEM 3



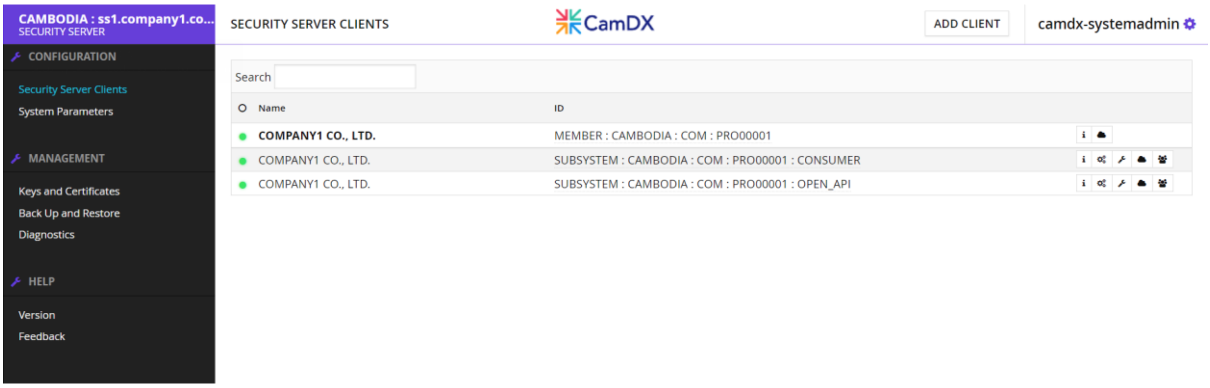
Name	ID
COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001
COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Do you want to send a client registration request for the added client?
New subsystem 'OPEN_API' will be submitted for registration for member 'COMPANY1 CO., LTD. COM: PRO00001'.

FIGURE 33 – ADD A SUBSYSTEM 4

In this scenario, the subsystem is a service provider sharing their "OPEN_API" (the subsystem code is provided by CamDXOperator) to the other CamDX members. The status is YELLOW pending approval from the CamDX Operator and will turn GREEN after the approval.

Repeat adding the subsystem "CONSUMER".



Name	ID
COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001
COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER
COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

FIGURE 34 – ADD A SUBSYSTEM 5

4.11 ADDING CERTIFICATE FOR TLS CONNECTION BETWEEN INFORMATION SYSTEM AND SECURITY SERVER

For demonstration, the open api to expose will be https://pumiapp.herokuapp.com/pumi/provinces so we download their certificate and upload to security server.

The Certificate of the Information System will need to be uploaded to the Security Server's Subsystem named "OPEN_API" for TLS connection.

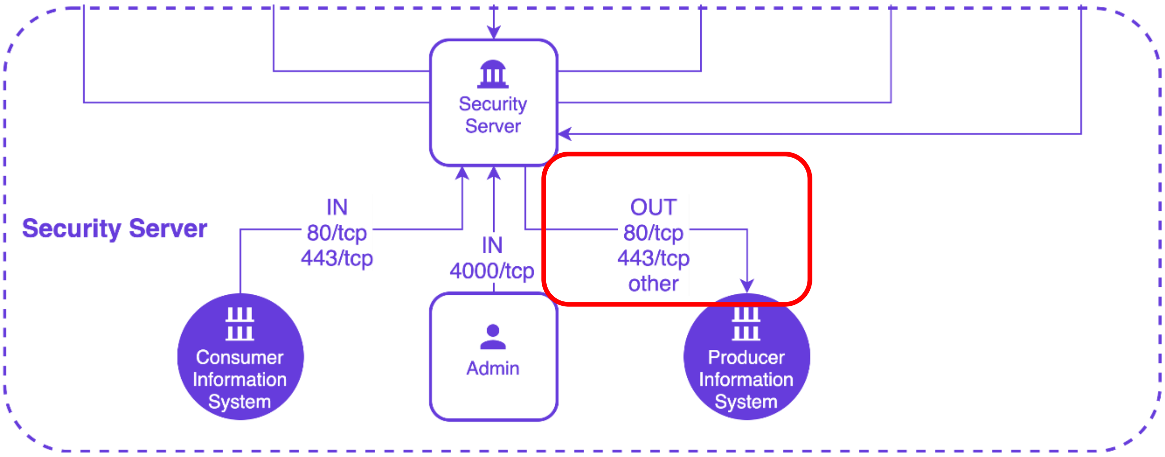
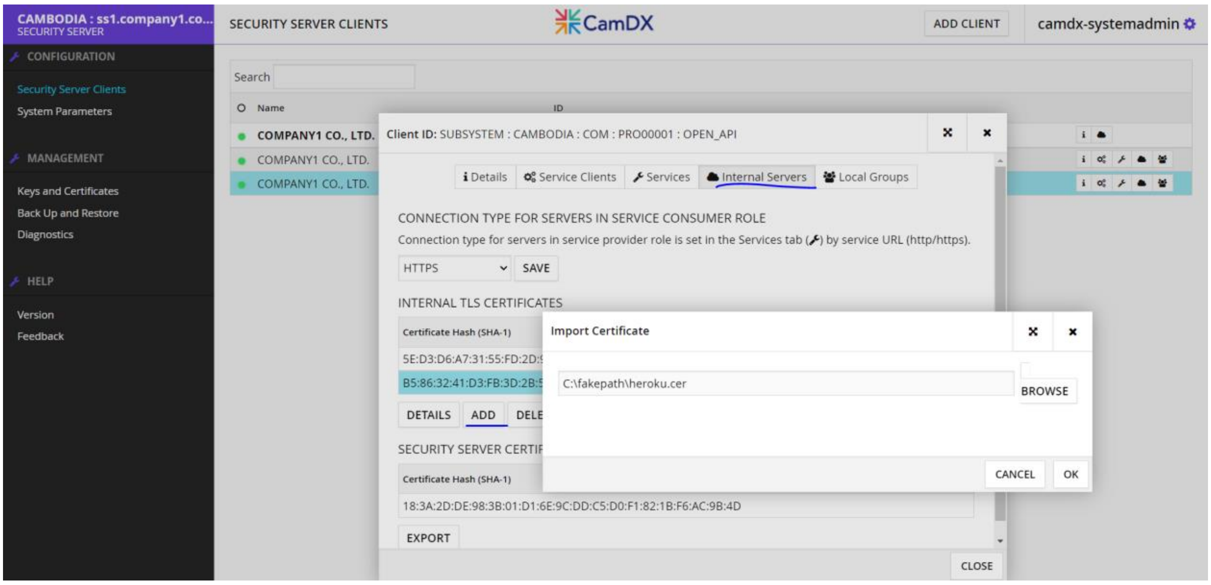


FIGURE 35 – ADDING TLS CERTIFICATE FOR INFORMATION SYSTEM

- Open Security Server Clients
    - Select **SUBSYSTEM**
    - Click **Internal Servers**
    - Press **ADD** at **INTERNAL TLS CERTIFICATES**



CAMBODIA : ss1.company1.co...
SECURITY SERVER

SECURITY SERVER CLIENTS

CamDX

ADD CLIENT

camdx-systemadmin

CONFIGURATION

Security Server Clients
System Parameters

MANAGEMENT

Keys and Certificates
Back Up and Restore
Diagnostics

HELP

Version
Feedback

Search

Name	ID
COMPANY1 CO., LTD.	
COMPANY1 CO., LTD.	
COMPANY1 CO., LTD.	

Client ID: SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Details | Service Clients | Services | Internal Servers | Local Groups

CONNECTION TYPE FOR SERVERS IN SERVICE CONSUMER ROLE

Connection type for servers in service provider role is set in the Services tab (🔧) by service URL (http/https).

HTTPS | SAVE

INTERNAL TLS CERTIFICATES

Certificate Hash (SHA-1)
5E:D3:D6:A7:31:55:FD:2D:
B5:86:32:41:D3:FB:3D:2B:

DETAILS | ADD | DELE

SECURITY SERVER CERTIF

Certificate Hash (SHA-1)
18:3A:2D:DE:98:3B:01:D1:6E:9C:DD:C5:D0:F1:82:1B:F6:AC:9B:4D

EXPORT

CLOSE

Import Certificate

C:\fakepath\heroku.cer

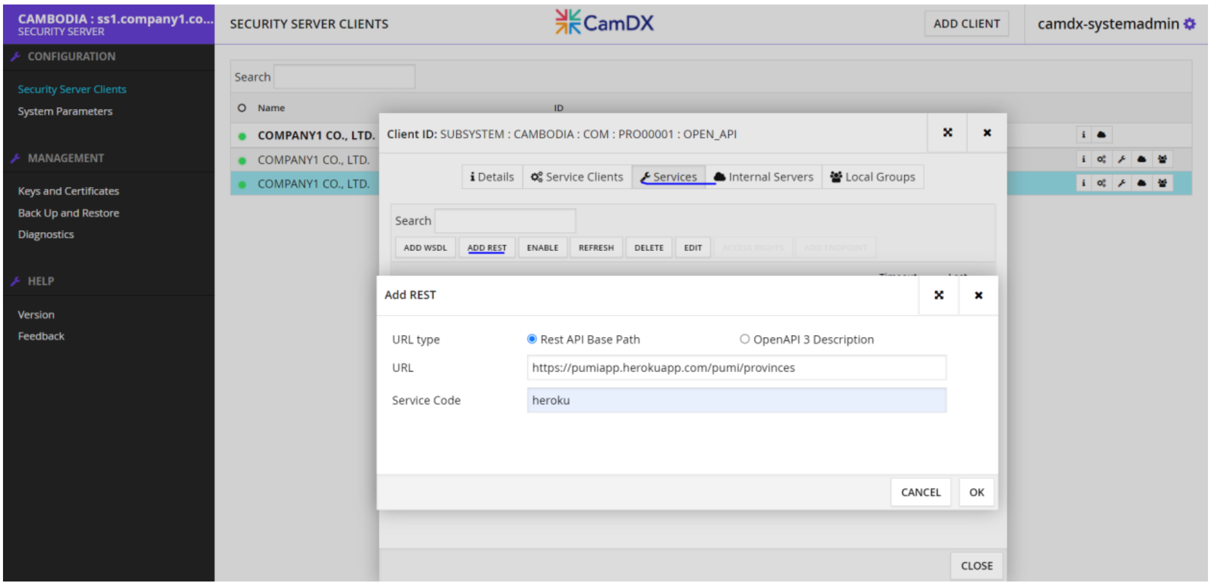
BROWSE

CANCEL | OK

FIGURE 36 – UPLOAD INFORMATION SYSTEM CERTIFICATE

4.12 ADDING A NEW SERVICE TO THE SUBSYSTEM “OPEN_API”

- Open Security Server Clients
  - Select **SUBSYSTEM**
  - Click **SERVICES**
    - Press **ADD REST**
    - Enter **URL** & **SERVICE CODE**
    - Press **OK**



CAMBODIA : ss1.company1.co...
SECURITY SERVER

SECURITY SERVER CLIENTS

CamDX

ADD CLIENT

camdx-systemadmin

CONFIGURATION

Security Server Clients
System Parameters

MANAGEMENT

Keys and Certificates
Back Up and Restore
Diagnostics

HELP

Version
Feedback

Search

Name	ID
COMPANY1 CO., LTD.	
COMPANY1 CO., LTD.	
COMPANY1 CO., LTD.	

Client ID: SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Details | Service Clients | Services | Internal Servers | Local Groups

Search

ADD WSDL | ADD REST | ENABLE | REFRESH | DELETE | EDIT

Add REST

URL type: ● Rest API Base Path ○ OpenAPI 3 Description

URL: https://pumiapp.herokuapp.com/pumi/provinces

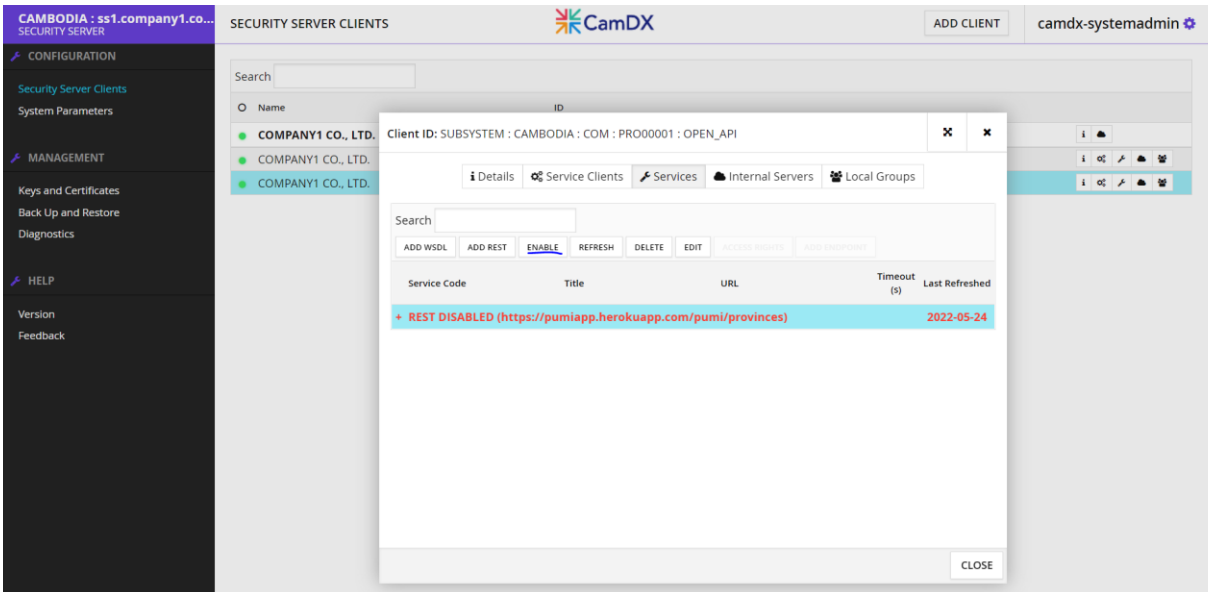
Service Code: heroku

CANCEL | OK

CLOSE

FIGURE 37 – ADDING A SERVICE TO SUBSYSTEM

- Select **SERVIC CODE** => Press **ENABLE**



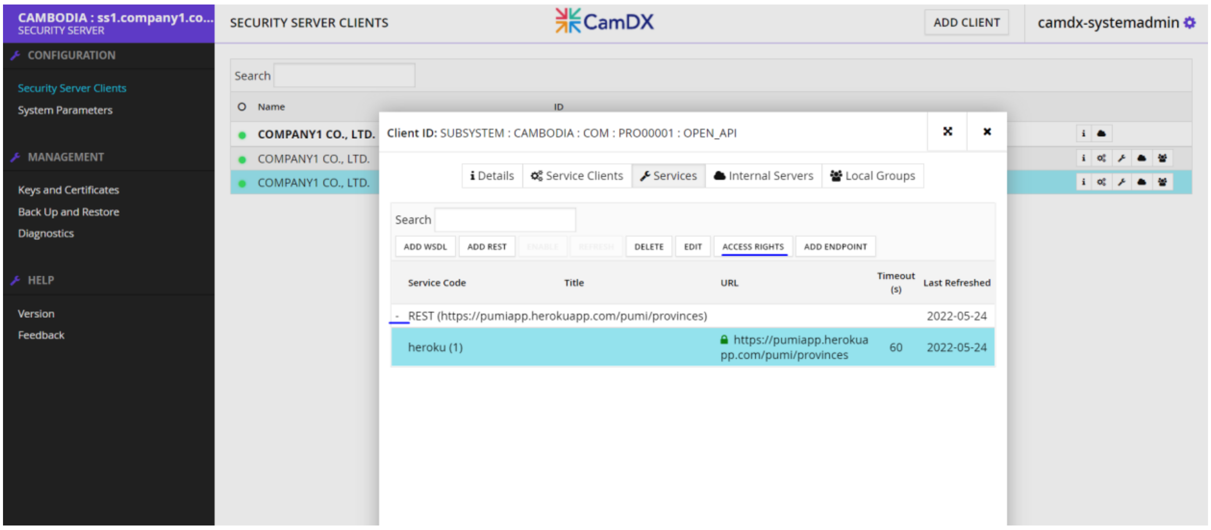
COMPANY1 CO., LTD.
COMPANY1 CO., LTD.
COMPANY1 CO., LTD.

Client ID: SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Service Code	Title	URL	Timeout (s)	Last Refreshed
+ REST DISABLED (https://pumiapp.herokuapp.com/pumi/provinces)				2022-05-24

FIGURE 38 – ENABLING SERVICE

- Click **+** to expand
    - Select **SERVICE CODE** – "heroku"
    - Press **ACCESS RIGHTS**
    - Press **ADD SUBJECTS**
    - Press **SEARCH**
    - Select "**CONSUMER**" to be added to the ACL
    - Press **ADD SELECTED TO ACL**

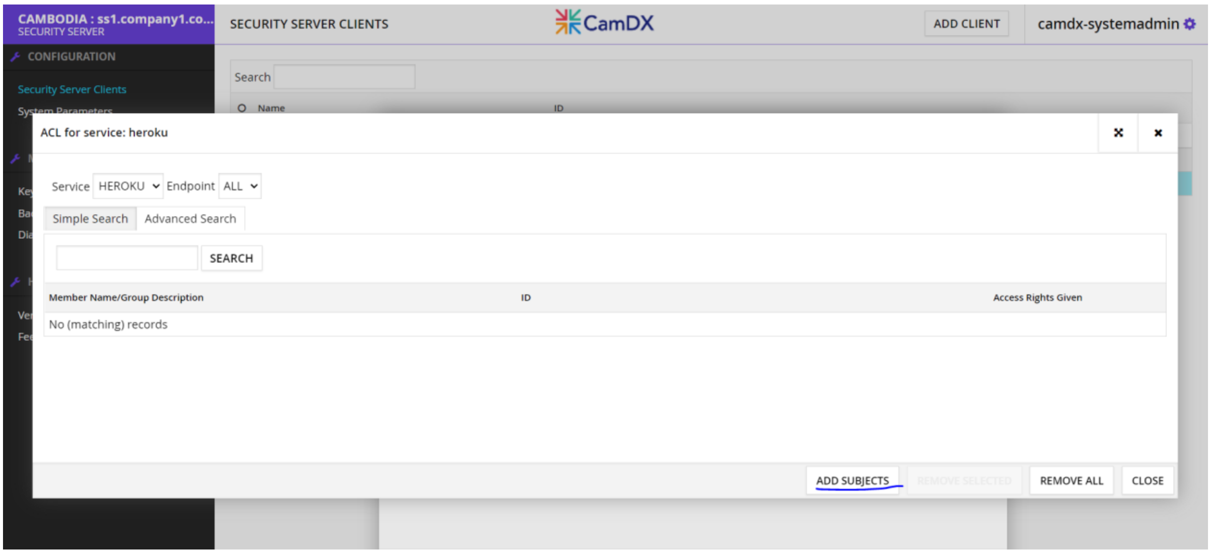


COMPANY1 CO., LTD.
COMPANY1 CO., LTD.
COMPANY1 CO., LTD.

Client ID: SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Service Code	Title	URL	Timeout (s)	Last Refreshed
- REST (https://pumiapp.herokuapp.com/pumi/provinces)				2022-05-24
heroku (1)		https://pumiapp.herokuapp.com/pumi/provinces	60	2022-05-24

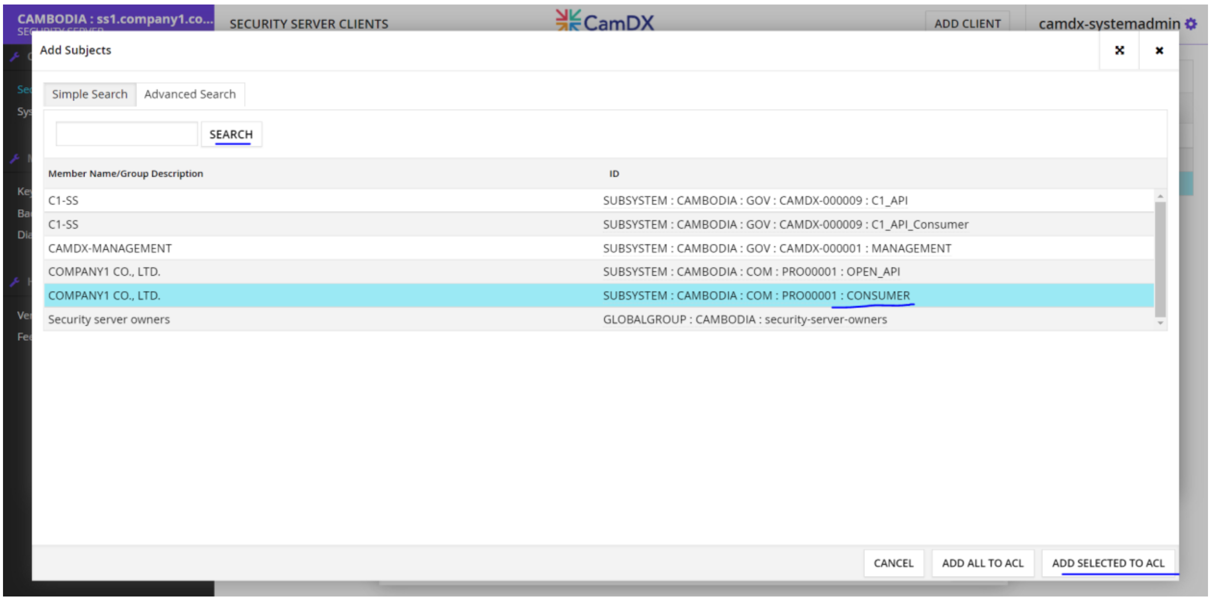
FIGURE 39 – ADDING SUBSYSTEM TO THE ACL



ACL for service: heroku

Member Name/Group Description	ID	Access Rights Given
No (matching) records		

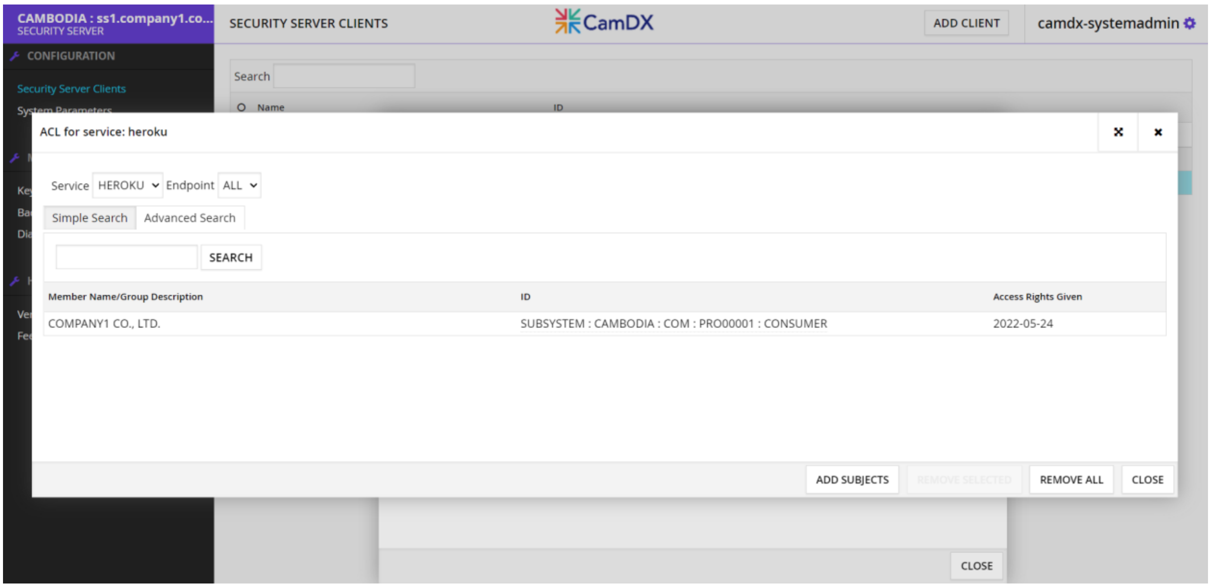
FIGURE 40 – ADDING SUBSYSTEM TO THE ACL 2



Add Subjects

Member Name/Group Description	ID
C1-SS	SUBSYSTEM : CAMBODIA : GOV : CAMDX-000009 : C1_API
C1-SS	SUBSYSTEM : CAMBODIA : GOV : CAMDX-000009 : C1_API_Consumer
CAMDX-MANAGEMENT	SUBSYSTEM : CAMBODIA : GOV : CAMDX-000001 : MANAGEMENT
COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API
COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER
Security server owners	GLOBALGROUP : CAMBODIA : security-server-owners

FIGURE 41 – ADDING SUBSYSTEM TO THE ACL 3



ACL for service: heroku

Member Name/Group Description	ID	Access Rights Given
COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER	2022-05-24

FIGURE 42 – ADDING SUBSYSTEM TO THE ACL 4

4.13 ADDING CERTIFICATE FOR TLS CONNECTION BETWEEN CONSUMER SYSTEM AND SECURITY SERVER

For demonstration purpose, the consumer system's certificate will be self-signed and upload to the Security Server's Subsystem named "CONSUMER" for TLS connection.

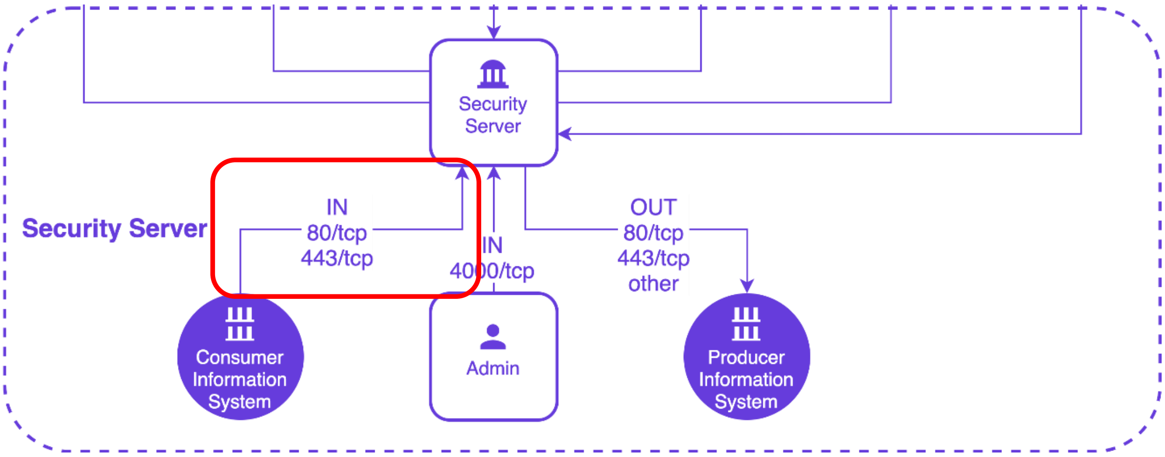
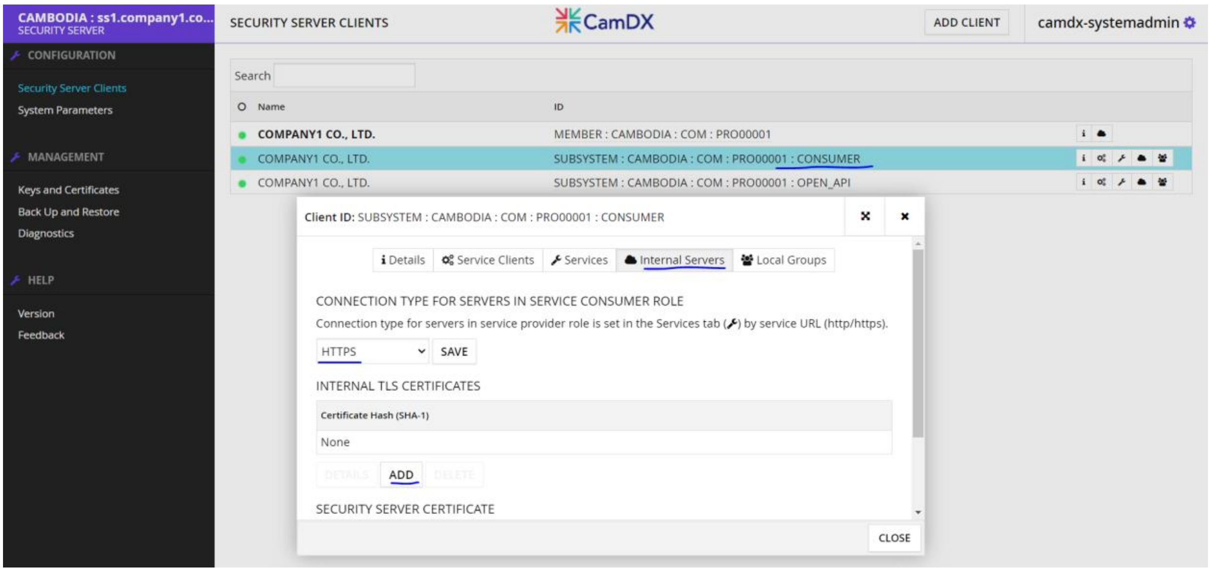


FIGURE 43 – ADDING TLS CERTIFICATE FOR INFORMATION SYSTEM

- Open Security Server Clients
  - Select **SUBSYSTEM - CONSUMER**
  - Click **Internal Servers**
  - Press **ADD** at **INTERNAL TLS CERTIFICATES**



Name	ID
● COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001
● COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER
● COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Client ID: SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER

CONNECTION TYPE FOR SERVERS IN SERVICE CONSUMER ROLE

Connection type for servers in service provider role is set in the Services tab (🔧) by service URL (http/https).

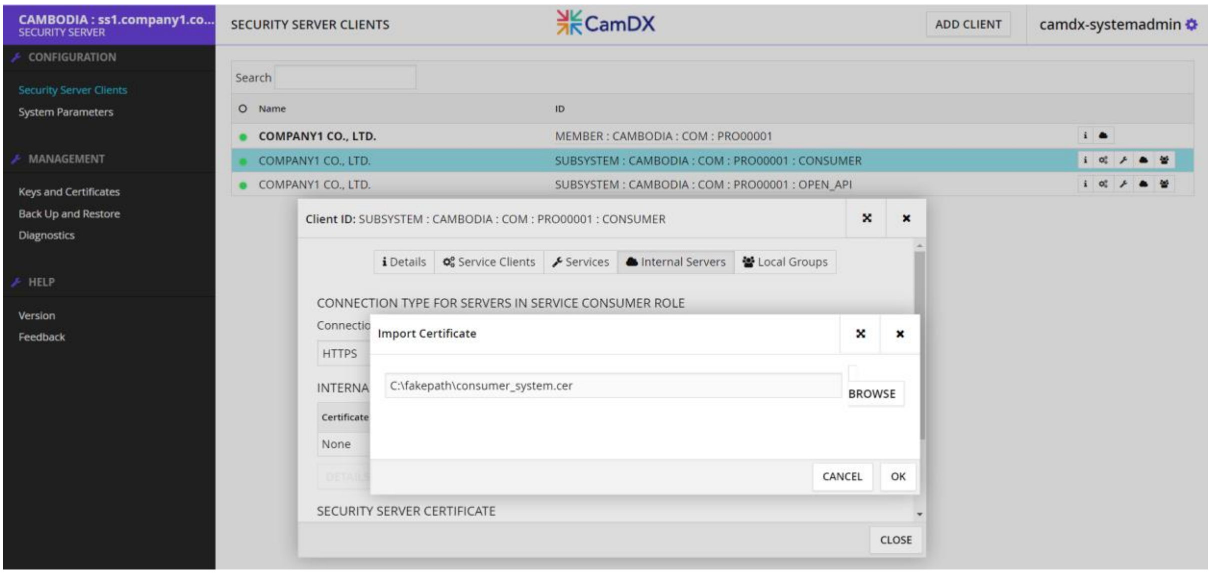
HTTPS

INTERNAL TLS CERTIFICATES

Certificate Hash (SHA-1)
None

SECURITY SERVER CERTIFICATE

FIGURE 44 – UPLOAD CONSUMER SYSTEM CERTIFICATE



CAMBODIA : ss1.company1.co...
SECURITY SERVER

CONFIGURATION
Security Server Clients
System Parameters

MANAGEMENT
Keys and Certificates
Back Up and Restore
Diagnostics

HELP
Version
Feedback

SECURITY SERVER CLIENTS — CamDX — ADD CLIENT — camdx-systemadmin

Search

	Name	ID
●	COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001
●	COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER
●	COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Client ID: SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER

Details | Service Clients | Services | Internal Servers | Local Groups

CONNECTION TYPE FOR SERVERS IN SERVICE CONSUMER ROLE

Connectio

HTTPS

INTERNA

Certificate

None

Import Certificate

C:\fakepath\consumer_system.cer

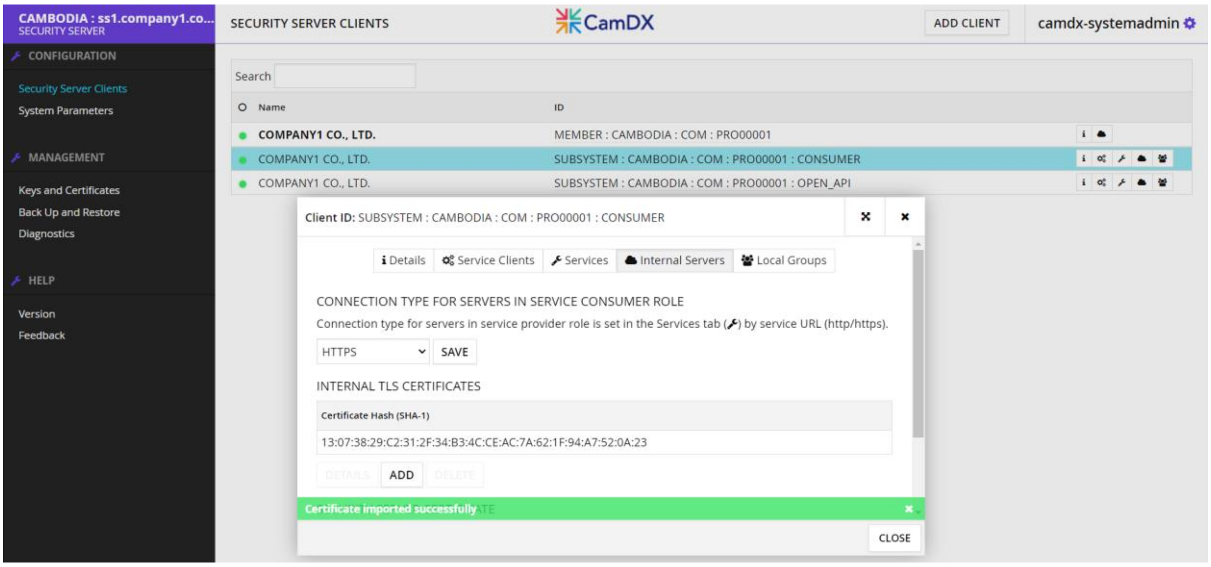
BROWSE

CANCEL OK

SECURITY SERVER CERTIFICATE

CLOSE

FIGURE 45 – UPLOAD CONSUMER SYSTEM CERTIFICATE 2



CAMBODIA : ss1.company1.co...
SECURITY SERVER

CONFIGURATION
Security Server Clients
System Parameters

MANAGEMENT
Keys and Certificates
Back Up and Restore
Diagnostics

HELP
Version
Feedback

SECURITY SERVER CLIENTS — CamDX — ADD CLIENT — camdx-systemadmin

Search

	Name	ID
●	COMPANY1 CO., LTD.	MEMBER : CAMBODIA : COM : PRO00001
●	COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER
●	COMPANY1 CO., LTD.	SUBSYSTEM : CAMBODIA : COM : PRO00001 : OPEN_API

Client ID: SUBSYSTEM : CAMBODIA : COM : PRO00001 : CONSUMER

Details | Service Clients | Services | Internal Servers | Local Groups

CONNECTION TYPE FOR SERVERS IN SERVICE CONSUMER ROLE

Connection type for servers in service provider role is set in the Services tab () by service URL (http/https).

HTTPS SAVE

INTERNAL TLS CERTIFICATES

Certificate Hash (SHA-1)
13:07:38:29:C2:31:2F:34:B3:4C:CE:AC:7A:62:1F:94:A7:52:0A:23

DETAILS ADD DELETE

Certificate imported successfully

CLOSE

FIGURE 46 – UPLOAD CONSUMER SYSTEM CERTIFICATE 3

4.14 ACCESS THE OPEN API

After all the setup and configuration, we may now access the OPEN_API subsystem from the CONSUMER subsystem via CamDX Data Exchange Layer.

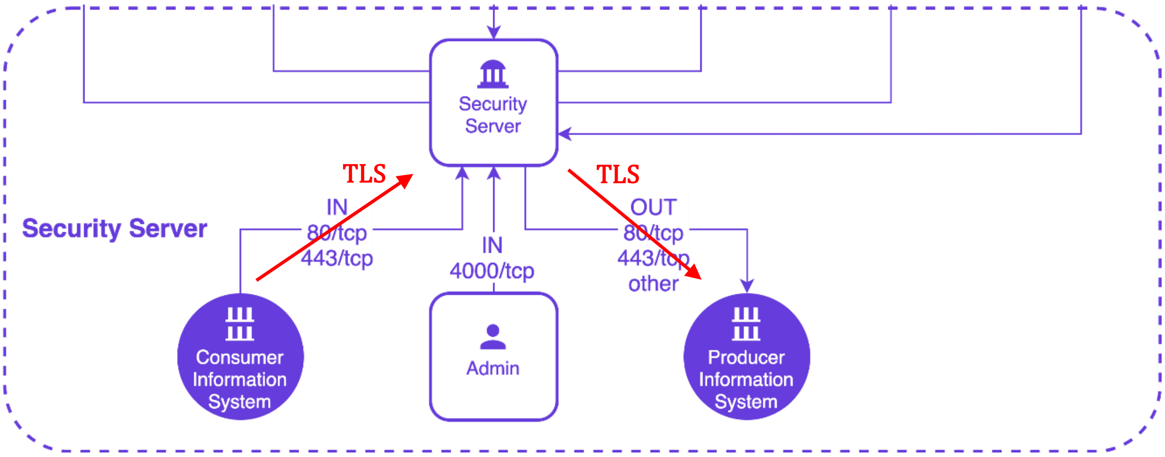
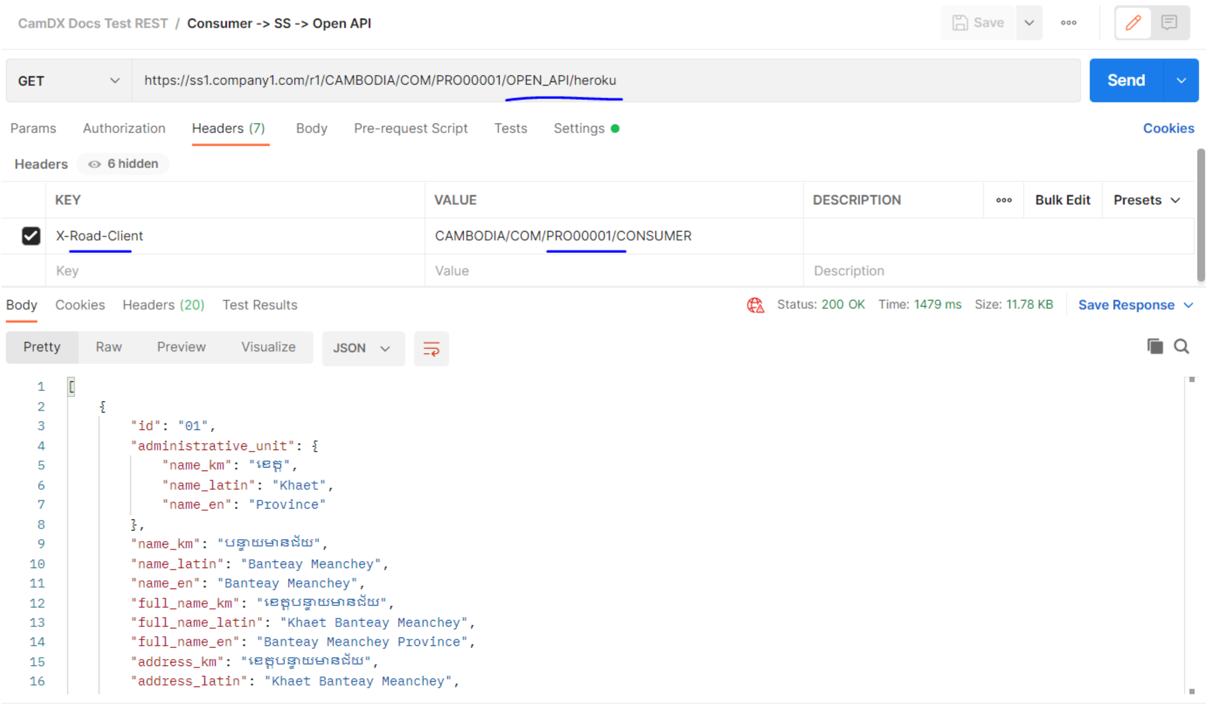


FIGURE 47 – ACCESSING OPEN_API

- GET https://ss1.company1.com/r1/CAMBODIA/COM/PRO00001/OPEN_API/heroku
- Header: **X-Road-Client:** CAMBODIA/COM/PRO00001/CONSUMER



https://ss1.company1.com/r1/CAMBODIA/COM/PRO00001/OPEN_API/heroku

	KEY	VALUE	DESCRIPTION
☑	X-Road-Client	CAMBODIA/COM/PRO00001/CONSUMER	
	Key	Value	Description

Status: 200 OK Time: 1479 ms Size: 11.78 KB

```
[
    {
        "id": "01",
        "administrative_unit": {
            "name_km": "ខេត្ត",
            "name_latin": "Khaet",
            "name_en": "Province"
        },
        "name_km": "បន្ទាយមានជ័យ",
        "name_latin": "Banteay Meanchey",
        "name_en": "Banteay Meanchey",
        "full_name_km": "ខេត្តបន្ទាយមានជ័យ",
        "full_name_latin": "Khaet Banteay Meanchey",
        "full_name_en": "Banteay Meanchey Province",
        "address_km": "ខេត្តបន្ទាយមានជ័យ",
        "address_latin": "Khaet Banteay Meanchey",
```

FIGURE 48 – ACCESSING OPEN_API 2

- https://ss1.company1.com/r1/ => Request from Security Server Member that was allowed in the ACL
- CAMBODIA/COM/PRO00001/OPEN_API/heroku => To Access Service "heroku" on Subsystem named "OPEN_API" of Security Server with Member Code "PRO00001"
- **X-Road-Client:** CAMBODIA/COM/PRO00001/CONSUMER => ID of Security Server's Subsystem allowed in the ACL

This looks a bit confusing since both subsystems are on the same security server. Let's see another scenario of two security server communication.

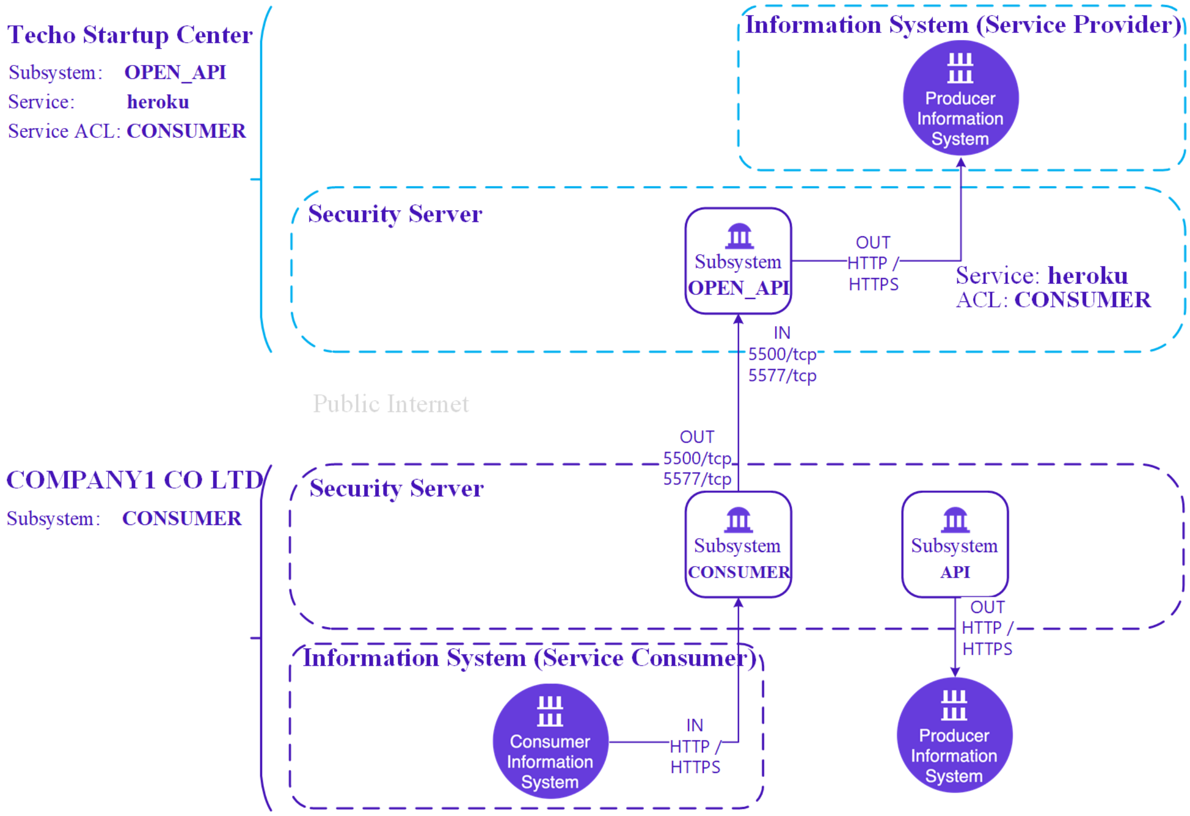
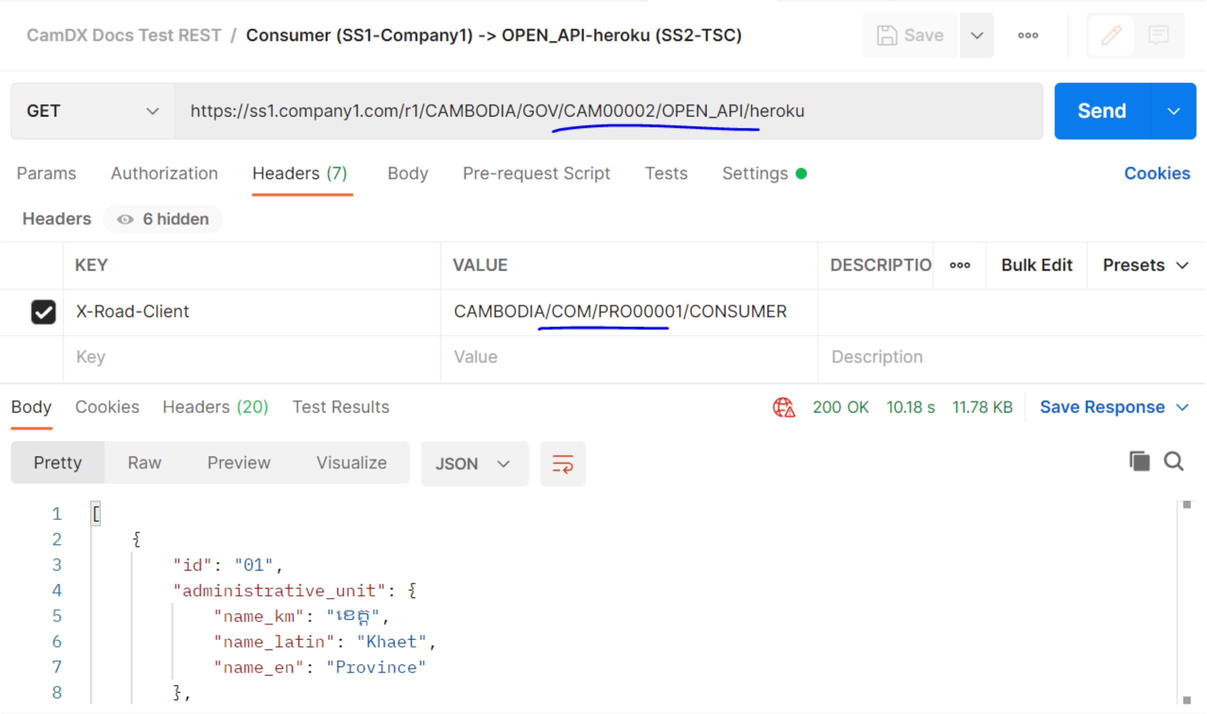


FIGURE 49 – SCENARIO 2 ACCESSING OPEN_API

This demo-scenario, the communication is between two Security Servers from different organization. The service provider organization is “Techo Startup Center” with Subsystem “OPEN_API” sharing Service named “heroku" and the service consumer organization is “COMPANY1 CO LTD” with Subsystem “CONSUMER” that was allowed the ACL of “heroku" service.



GET https://ss1.company1.com/r1/CAMBODIA/GOV/CAM00002/OPEN_API/heroku

	KEY	VALUE	DESCRIPTIO
☑	X-Road-Client	CAMBODIA/COM/PRO00001/CONSUMER	
	Key	Value	Description

200 OK 10.18 s 11.78 KB

```
[
    {
        "id": "01",
        "administrative_unit": {
            "name_km": "ខេត្ត",
            "name_latin": "Khaet",
            "name_en": "Province"
        },
```

FIGURE 50 – SCENARIO 2 ACCESSING OPEN_API 2

- https://ss1.company1.com/r1/ => Request from Security Server Member that was allowed in the ACL
- CAMBODIA/GOV/CAM00002/OPEN_API/heroku => To Access Service “heroku” on Subsystem named “OPEN_API” of Security Server with Member Code “CAM00002”.
- **X-Road-Client:** CAMBODIA/COM/PRO00001/CONSUMER => ID of Security Server’s Subsystem allowed in the ACL of service “heroku”

5. COMMANDS USED

```
sudo apt update
sudo apt upgrade
sudo timedatectl set-timezone Asia/Phnom_Penh
sudo adduser camdx-systemadmin
echo LC_ALL=en_US.UTF-8 | sudo tee -a /etc/environment
sudo apt-get install locales software-properties-common
curl http://repository.camdx.gov.kh/repository/camdx-anchors/api/gpg/key/0x04194DBF-pub.asc | sudo apt-key add -
echo deb [arch=all,amd64] http://repository.camdx.gov.kh/repository/camdx-release bionic main | sudo tee -a /etc/apt/sources.list
sudo apt-get update
sudo apt-get install xroad-securityserver
sudo apt install xroad-addon-proxymonitor
sudo apt install xroad-addon-opmonitoring
sudo systemctl restart xroad-opmonitor
```

6. REFERENCES

X-Road/ig-ss_x-road_v6_security_server_installation_guide.md at camdx-6.23.0 · CamDX/X-Road. (2022). Retrieved 26 May 2022, from https://github.com/CamDX/X-Road/blob/camdx-6.23.0/doc/Manuals/ig-ss_x-road_v6_security_server_installation_guide.md

HIGH AVAILABILITY SECURITY SERVER INSTALLATION WITH EXTERNAL LOAD BALANCER

By CamDX Operator

July 2022

DOCUMENT VERSION HISTORY

RELEASE NO	AUTHOR	DATE	BRIEF SUMMARY OF CHANGES
V1.0.0	CamDX Operator	JULY 2022	

Contents

TABLES

Figures

7. SECURITY SERVER REQUIREMENT

7.1 Hardware: (Minimum Recommended)

- CPU: 64-bit dual-core Intel
- RAM: 4GB
- Network Card: 100 Mbps

7.2 Software:

- Operating System: Ubuntu 18.04 LTS x86-64
    - Add System User
        - **sudo adduser camdx-systemadmin**
- Set the operating system locale.
    - Add following line to the **/etc/environment.**
        - **LC_ALL=en_US.UTF-8**
- Ensure that the packages locales and software-properties-common are present
    - **sudo apt-get install locales software-properties-common**
- Ensure that the timezone is set to Asia/Phnom_Penh – timedatectl
    - **sudo timedatectl set-timezone Asia/Phnom_Penh**

7.3 Network Ports

It is strongly recommended to protect the security server from unwanted access using a firewall (hardware or software based). The firewall can be applied to both incoming and outgoing connections depending on the security requirements of the environment where the security server is deployed. It is recommended to allow incoming traffic to specific ports only from explicitly defined sources using IP filtering. Special attention should be paid with the firewall configuration since incorrect configuration may leave the security server vulnerable to exploits and attacks.

The table below lists the required connections between different components.

Connection Type	Source	Target	Target Ports	Protocol	Note
Out	Security Server	Central Server	80, 4001	tcp	
Out	Security Server	Management Security Server	5500, 5577	tcp	
Out	Security Server	OCSP Service	80 / 443	tcp	
Out	Security Server	Timestamping Service	80 / 443	tcp	
Out	Security Server	Data Exchange Partner Security Server (Service Producer)	5500, 5577	tcp	
Out	Security Server	Producer Information System	80, 443, other	tcp	Target in the internal network

Connection Type	Source	Target	Target Ports	Protocol	Note
In	Monitoring Security Server	Security Server	5500, 5577	tcp	
In	Data Exchange Partner Security Server (Service Consumer)	Security Server	5500, 5577	tcp	
In	Consumer Information System	Security Server	80, 443	tcp	Source in the internal network
In	Admin	Security Server	4000	tcp	Source in the internal network

TABLE 4 – NETWORK PORTS

7.4 Network Diagram

The network diagram below provides an example of HA Security Server setup with External Load Balancer.

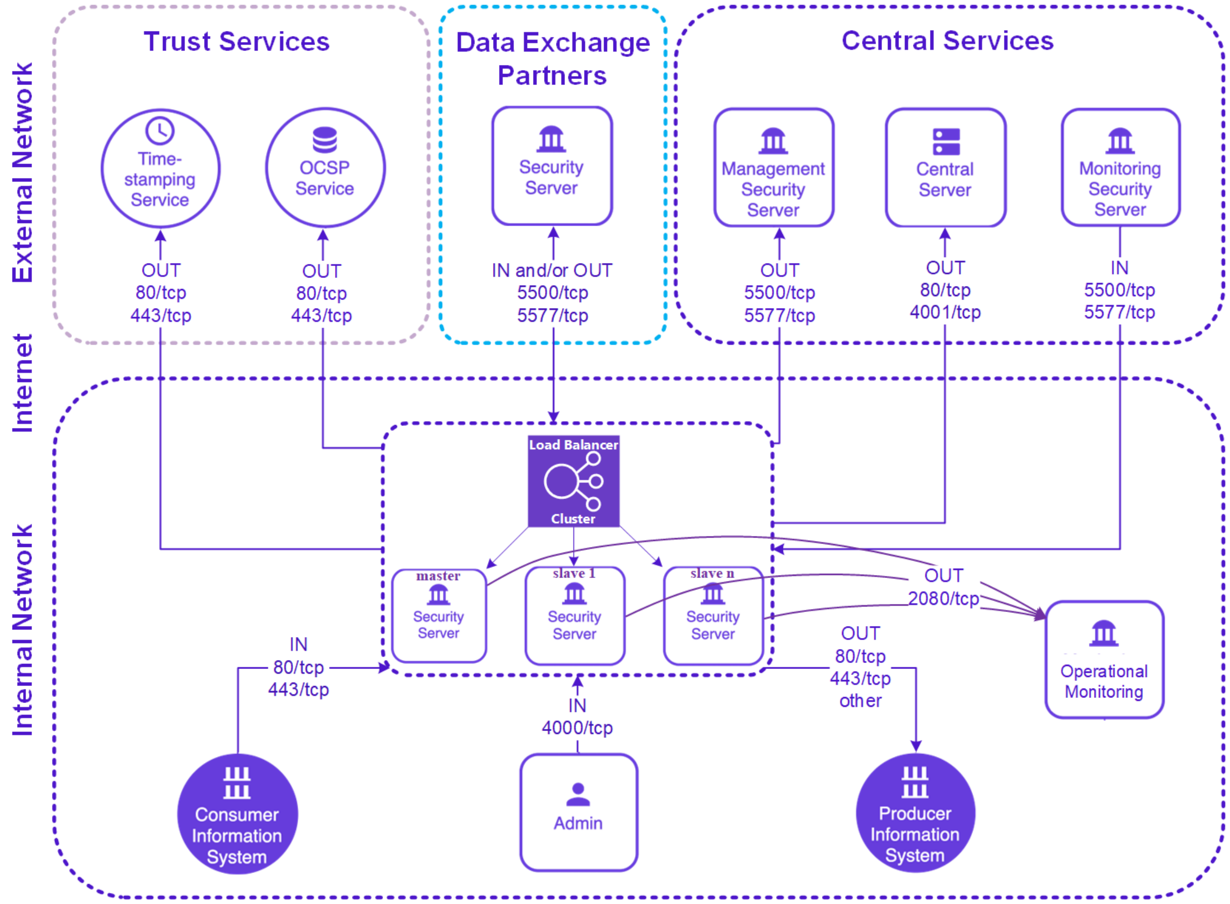


FIGURE 51 – NETWORK DIAGRAM

8. OVERVIEW

8.1 Inbound Request from Other Member

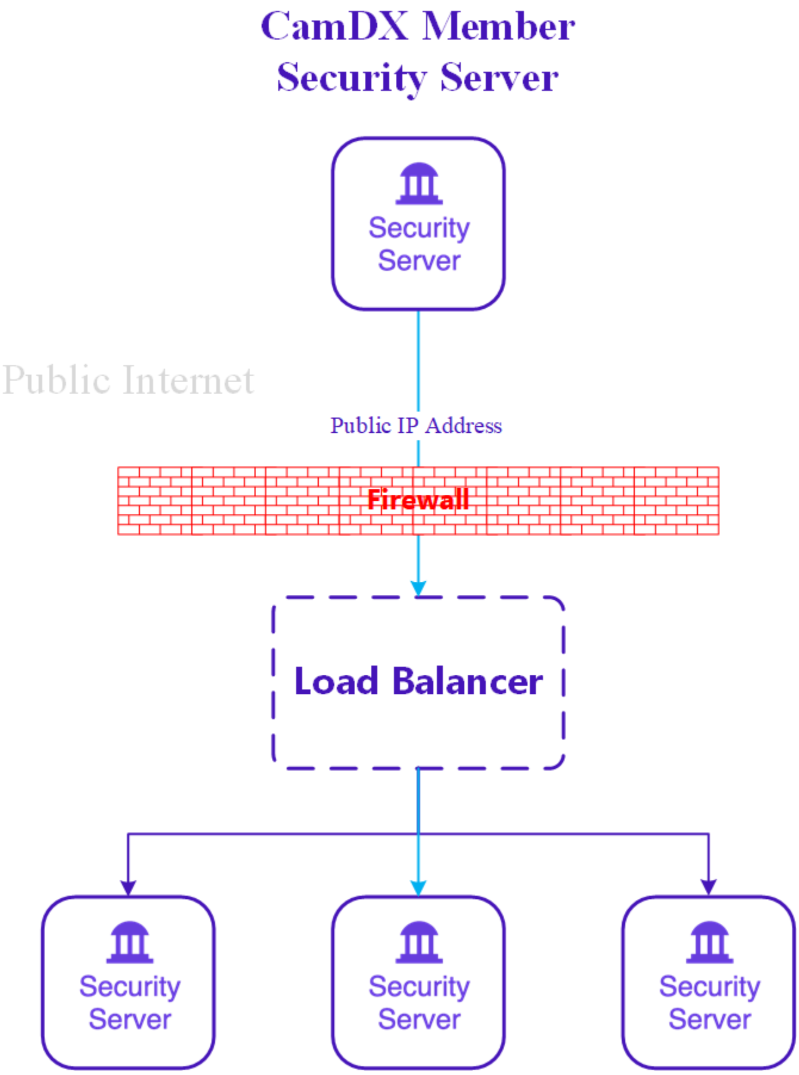


FIGURE 52 – INBOUND REQUEST

8.2 Outbound Request to Other Member

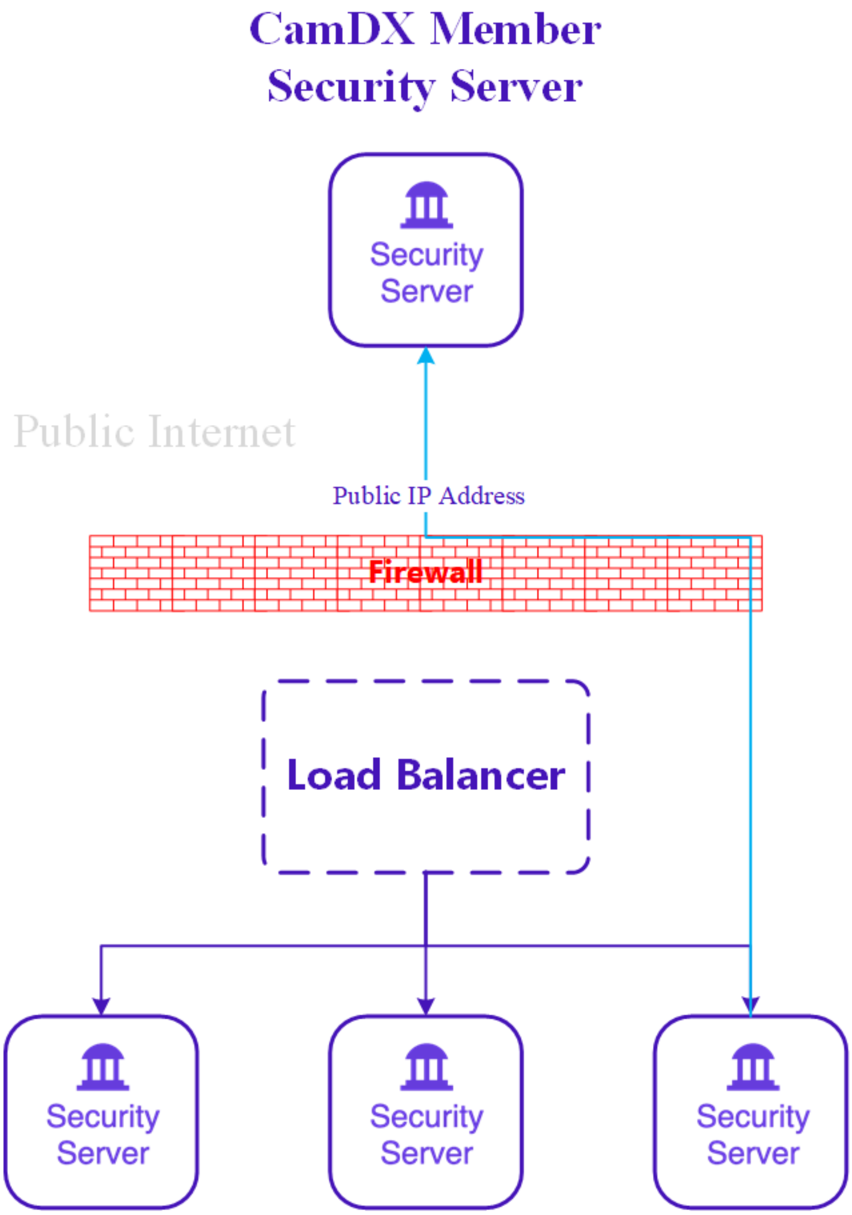


FIGURE 53 – OUTBOUND REQUEST

8.3 State Replication from Master Security Server to Slaves

- State Replication from the master to the slaves
- Replicated State:
    - **severconf** DB: PostgreSQL streaming replication (Hot standby),
    - **keyconf** replication(**softtoken** & **keyconf**): **rsync+ssh** (scheduled)
    - Other server configuration parameters from /etc/xroad/*: **rsync+ssh** (schedule)
        - db.properties
        - postgresql/*
        - globalconf/
        - conf.d/node.ini
- Non-replicated State:
    - **messagelog** DB
    - OCSP responses from **/var/cache/xroad**

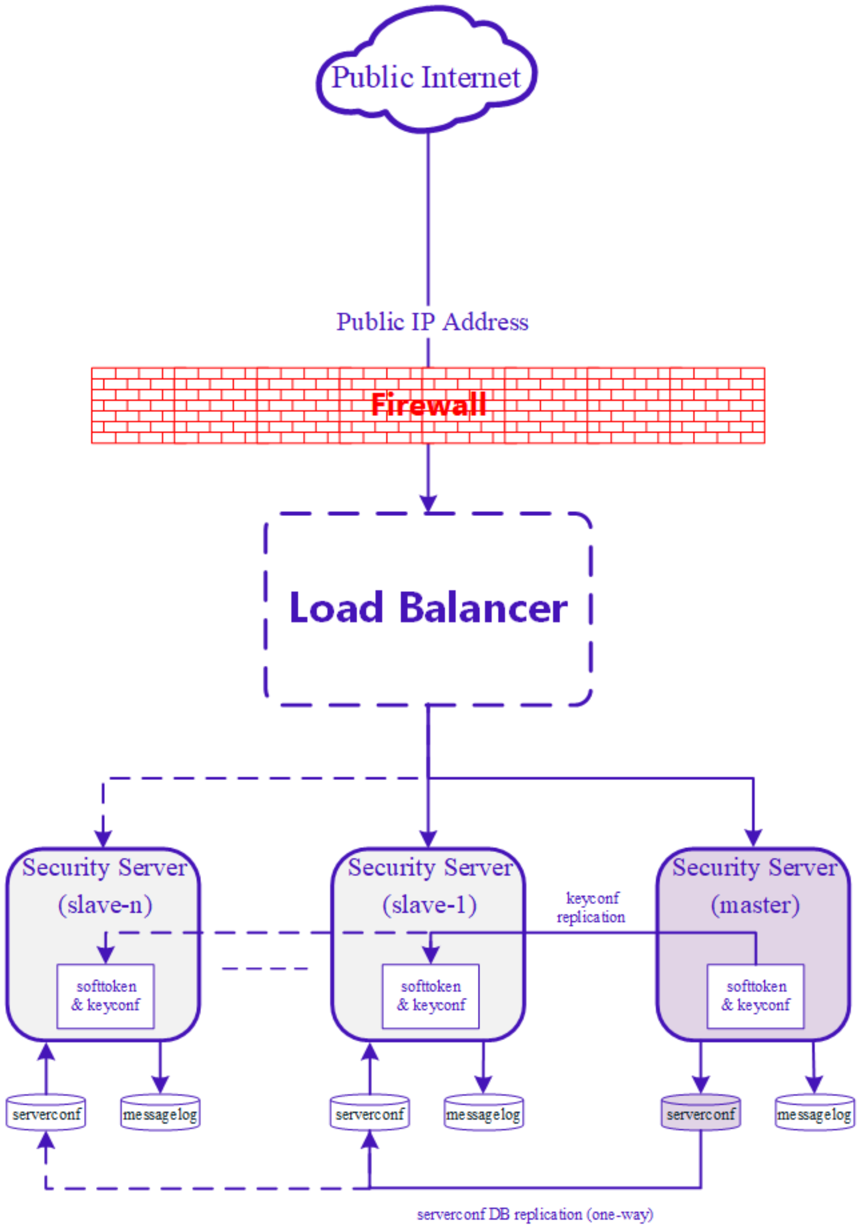


FIGURE 54 – MASTER SLAVES STATE REPLICATION

9. INSTALLATION

9.1 Prerequisites

In order to properly setup data replication, the slave nodes must be able to connect to:

- The **master server** using SSH (tcp port 22), and
- The **master serverconf** database (e.g tcp port 5433)

9.2 Master Installation Steps

- Install the CamDX Security Server packages using the normal installation guideline or use an existing standalone node.
- Stop the CamDX Security Server services. By using command: **sudo systemctl stop "xroad-*"**
- Data Replication Setup - Create a separate PostgreSQL instance for the **serverconf** database
- Change **/etc/xroad/db.properties** to point to the separate database instance
  - **serverconf.hibernate.connection.url**: change the url port number from **5432** to **5433** (or the port you specified)
  - **serverconf.hibernate.connection.password**: Change to match the master db's password (in plaintext)
- **Data Replication Setup** - Configuration file replication (3.4.1, 3.4.3, 3.4.4)
- Configure the node type as **master** in **/etc/xroad/conf.d/node.ini**
  - **[node]**
  - **type=master**
- Change the owner and group of the file to **xroad:xroad** if it is not already
- Start the CamDX Security Server services

9.3 Slave Installation Steps

- Install the CamDX Security Server packages using the normal installation guideline or use an existing standalone node.
- Stop the CamDX Security Server services. By using command: **sudo systemctl stop "xroad-*"**
- **Data Replication Setup** - Create a separate PostgreSQL instance for the **serverconf** database
- Change /etc/xroad/db.properties to point to the separate database instance
  - **serverconf.hibernate.connection.url**: change the url port number from **5432** to **5433** (or the port you specified)
  - **serverconf.hibernate.connection.password**: Change to match the master db's password (in plaintext)
- **Data Replication Setup** - Configuration file replication (3.4.2, 3.4.3, 3.4.4)
- Configure the node type as **master** in **/etc/xroad/conf.d/node.ini**
  - **[node]**
  - **type=slave**
- Change the owner and group of the file to **xroad:xroad** if it is not already
- Start the CamDX Security Server services

9.4 Data Replication Setup

9.4.1 Create a Separate PostgreSQL Instance for serverconf Database on Master Node

#Setting up TLS Certificate for Database Authentication:

##Generate the Certificate Authority Key and a self-signed Certificate for the root-of-trust

```
openssl req -new -x509 -days 7300 -nodes -sha256 -out ca.crt -keyout ca.key -subj '/O=COMPANY1 CO LTD/CN=CA'
```

##Generate Keys and Certificates signed by the CA for each PostgreSQL Instance, including the master. Do not use the CA certificate and key as the database certificate and key

```
openssl req -new -nodes -days 7300 -keyout server.key -out server.csr -subj "/O=COMPANY1 CO LTD/CN=ss1.company1.com"
openssl x509 -req -in server.csr -CAcreateserial -CA ca.crt -CAkey ca.key -days 7300 -out server.crt
```

##Copy the Certificates and Keys

```
sudo mkdir -p -m 0755 /etc/xroad/postgresql
sudo chmod o+x /etc/xroad
sudo cp ca.crt server.crt server.key /etc/xroad/postgresql
sudo chown postgres /etc/xroad/postgresql/*
sudo chmod 400 /etc/xroad/postgresql/*
```

#Create a serverconf database by using the following command:

```
sudo -u postgres pg_createcluster -p 5433 10 serverconf
```

#Configuring the master instance for replication:

```
sudo vim /etc/postgresql/10/serverconf/postgresql.conf
    ssl = on
    ssl_ca_file   = '/etc/xroad/postgresql/ca.crt'
    ssl_cert_file = '/etc/xroad/postgresql/server.crt'
    ssl_key_file  = '/etc/xroad/postgresql/server.key'

    listen_addresses = '*'    # (default is localhost. Alternatively: localhost, <IP of the interface the slaves connect to>")
    wal_level = hot_standby
    max_wal_senders   = 3   # should be ~ number of slaves plus some small number. Here, we assume there are two slave
    wal_keep_segments = 8   # keep some wal segments so that slaves that are offline can catch up.
```

```
sudo vim /etc/postgresql/10/serverconf/pg_hba.conf
    hostssl    replication    +slavenode  samenet    cert
```

```
systemctl start postgresql@10-serverconf
sudo -u postgres psql -p 5433 -c "CREATE ROLE slavenode NOLOGIN";
sudo -u postgres psql -p 5433 -c "CREATE USER "ss2" REPLICATION PASSWORD NULL IN ROLE slavenode";
sudo -u postgres psql -p 5433 -c "CREATE USER serverconf PASSWORD '<password>'";
sudo -u postgres pg_dump -C serverconf | sudo -u postgres psql -p 5433 -f –
sudo -u postgres psql -p 5432 -c "ALTER DATABASE serverconf RENAME TO serverconf_old";
sudo vim /etc/xroad/db.properties
    serverconf.hibernate.connection.url = jdbc:postgresql://127.0.0.1:5433/serverconf
    serverconf.hibernate.connection.password = <Passw0rd>
```

#TLS Certificate for Database Authentication for Slave

##Generate the Certificate Authority Key and Certificate Signing Request

```
openssl req -new -nodes -days 7300 -keyout server_ss2.key -out server_ss2.csr -subj "/O=COMPANY1 CO LTD/CN=ss2"
openssl x509 -req -in server_ss2.csr -CAcreateserial -CA ca.crt -CAkey ca.key -days 7300 -out server_ss2.crt
```

9.4.2 Create a Separate PostgreSQL Instance for serverconf Database on Slave Node

```
#Setting up TLS Certificate for Database Authentication:
##Generate Keys and Certificates signed by the CA for each PostgreSQL Instance, including the master. Do not use
the CA certificate and key as the database certificate and key
sudo mkdir -p -m 0755 /etc/xroad/postgresql
sudo chmod o+x /etc/xroad

##Copy certificates and key from Master to Slave
sudo scp ca.crt server_ss2.crt server_ss2.key ss2@ip_of_ss_slave/home/ss2        #on Master Node
sudo mv ca.crt server_ss2.crt server_ss2.key /etc/xroad/postgresql
sudo chown postgres /etc/xroad/postgresql/*
sudo chmod 400 /etc/xroad/postgresql/*

#Create a serverconf database by using the following command:
sudo -u postgres pg_createcluster -p 5433 10 serverconf

#Configuring the slave instance for replication:
sudo -i
cd /var/lib/postgresql/10/serverconf
sudo rm -rf *
sudo -u postgres PGSSLMODE=verify-ca PGSSLROOTCERT=/etc/xroad/postgresql/ca.crt
PGSSLCERT=/etc/xroad/postgresql/server_ss2.crt PGSSLKEY=/etc/xroad/postgresql/server_ss2.key
pg_basebackup -h ip_of_ss_master -p 5433 -U ss2 -D .

sudo vim recovery.conf
    standby_mode = 'on'

    primary_conninfo = 'host=ip_of_ss_master port=5433 user=ss2 sslmode=verify-ca
    sslcert=/etc/xroad/postgresql/server_ss2.crt sslkey=/etc/xroad/postgresql/server_ss2.key
    sslrootcert=/etc/xroad/postgresql/ca.crt'

    trigger_file = '/var/lib/xroad/postgresql.trigger'



sudo chown postgres:postgres recovery.conf
sudo chmod 0600 recovery.conf
sudo vim /etc/postgresql/10/serverconf/postgresql.conf
    ssl = on
    ssl_ca_file   = '/etc/xroad/postgresql/ca.crt'
    ssl_cert_file = '/etc/xroad/postgresql/server_ss2.crt'
    ssl_key_file  = '/etc/xroad/postgresql/server_ss2.key'

    listen_addresses = localhost

    hot_standby = on
    hot_standby_feedback = on


sudo systemctl start postgresql@10-serverconf
sudo vim /etc/xroad/db.properties
    serverconf.hibernate.connection.url = jdbc:postgresql://127.0.0.1:5433/serverconf
    serverconf.hibernate.connection.password = <Passw0rd>
```

9.4.3 Setup SSH between slaves and master

```
#On slave, generate the ssh key for the xroad user by using the following command: (without a passphrase)
sudo -i -u xroad
sudo ssh-keygen -t rsa
#Copy ssh xroad public key to the Master Node for later adding to /home/xroad-slave/.ssh/authorized_keys
cat /var/lib/xroad/.ssh/id_rsa.pub

#On Master, setup a system user that can read /etc/xroad a system user has their password disabled and cannot log
in normally
sudo adduser --system --shell /bin/bash --ingroup xroad xroad-slave
sudo mkdir -m 755 -p /home/xroad-slave/.ssh && sudo touch /home/xroad-slave/.ssh/authorized_keys
#paste the copied id_rsa.pub from SS2
sudo vim /home/xroad-slave/.ssh/authorized_keys

#On slave, ssh to master with password with user xroad-slave
xroad@ss2# ssh xroad-slave@ip_of_ss_master
#Setup periodic configuration synchronization on the slave node (as root)
sudo vim /etc/systemd/system/xroad-sync.service
    [Unit]
    Description=X-Road Sync Task
    After=network.target
    Before=xroad-proxy.service
    Before=xroad-signer.service
    Before=xroad-confclient.service
    Before=xroad-jetty.service

    [Service]
    User=xroad
    Group=xroad
    Type=oneshot
    Environment=XROAD_USER=xroad-slave
    Environment=MASTER=ip_of_ss_master

    ExecStartPre=/usr/bin/test ! -f /var/tmp/xroad/sync-disabled

    ExecStart=/usr/bin/rsync -e "ssh -o ConnectTimeout=5 " -aqz --timeout=10 --delete-delay --exclude db.properties --exc
    "/conf.d/node.ini" --exclude "*.tmp" --exclude "/postgresql" --exclude "/nginx" --exclude "/globalconf" --exclude "/jett
    delay-updates --log-file=/var/log/xroad/slave-sync.log ${XROAD_USER}@${MASTER}:/etc/xroad/ /etc/xroad/

    [Install]
    WantedBy=multi-user.target
    WantedBy=xroad-proxy.service


sudo vim /etc/systemd/system/xroad-sync.timer
    [Unit]
    Description=Sync X-Road configuration
    [Timer]
    OnBootSec=60
    OnUnitActiveSec=60
    [Install]
    WantedBy=timers.target


sudo systemctl enable xroad-sync.timer xroad-sync.service          #enable and start service
sudo systemctl start xroad-sync.timer
sudo systemctl status xroad-sync.timer          #check service status
sudo systemctl status xroad-sync.service
sudo vim /etc/logrotate.d/xroad-slave-sync
    /var/log/xroad/slave-sync.log {
        daily
        rotate 7
        missingok
        compress
        su xroad xroad
        nocreate
    }
```

9.4.4 Configure Node Type: (Both Master and Slave)

```
sudo vim /etc/xroad/conf.d/node.ini     #on master
    [node]
    type=master

sudo chown xroad:xroad /etc/xroad/conf.d/node.ini
sudo systemctl start "xroad-*"


sudo vim /etc/xroad/conf.d/node.ini     #on slave
    [node]
    type=slave

sudo chown xroad:xroad /etc/xroad/conf.d/node.ini
sudo systemctl start "xroad-*"
```

9.5 Setup Verification

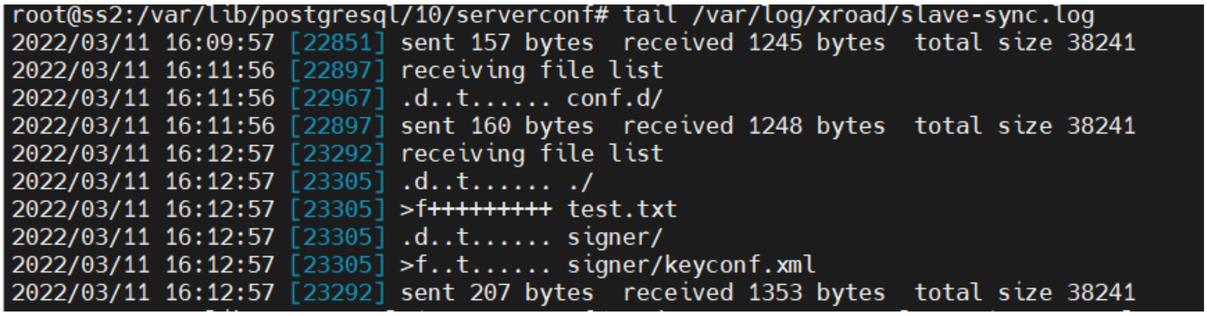
9.5.1 Verifying rsync+ssh replication:

To test the configuration file replication, a new file can be added to **/etc/xroad** or **/etc/xroad/signer** on the **master** node and verify it has been **replicated** to the **slave** nodes in a few minutes. Make sure the file is owned by the group xroad.

```
touch /etc/xroad/test.txt
chown xroad:xroad /etc/xroad/test.txt
```

Alternatively, check the sync log /var/log/xroad/slave-sync.log on the slave nodes and verifying its lists successful transfers.

```
tail /var/log/xroad/slave-sync.log
```

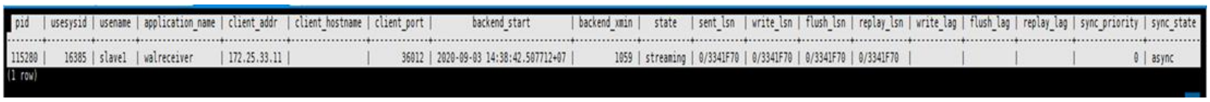


```
root@ss2:/var/lib/postgresql/10/serverconf# tail /var/log/xroad/slave-sync.log
2022/03/11 16:09:57 [22851] sent 157 bytes  received 1245 bytes  total size 38241
2022/03/11 16:11:56 [22897] receiving file list
2022/03/11 16:11:56 [22967] .d..t...... conf.d/
2022/03/11 16:11:56 [22897] sent 160 bytes  received 1248 bytes  total size 38241
2022/03/11 16:12:57 [23292] receiving file list
2022/03/11 16:12:57 [23305] .d..t...... ./
2022/03/11 16:12:57 [23305] >f+++++++++ test.txt
2022/03/11 16:12:57 [23305] .d..t...... signer/
2022/03/11 16:12:57 [23305] >f..t...... signer/keyconf.xml
2022/03/11 16:12:57 [23292] sent 207 bytes  received 1353 bytes  total size 38241
```

FIGURE 55 – VERIFY RSYNC

9.5.2 Verifying database replication: on Master

```
sudo -u postgres psql -p 5433 -c "select * from pg_stat_replication;"
```



```
 pid   | usesysid | usename | application_name | client_addr  | client_hostname | client_port |         backend_start          | backend_xmin |   state   | sent_lsn  | write_lsn | flush_lsn | replay_lsn | write_lag | flush_lag | replay_lag | sync_priority | sync_state
--------+----------+---------+------------------+--------------+-----------------+-------------+-------------------------------+--------------+-----------+-----------+-----------+-----------+------------+-----------+-----------+------------+---------------+------------
 115280 |    16385 | slave1  | walreceiver      | 172.25.33.11 |                 |       36012 | 2020-09-03 14:38:42.507712+07 |         1059 | streaming | 0/3341F70 | 0/3341F70 | 0/3341F70 | 0/3341F70  |           |           |            |             0 | async
(1 row)
```

FIGURE 56 – VERIFY DATABASE REPLICATION

10. EXTERNAL LOAD BALANCER (NGINX)

10.1 INSTALLATION AND CONFIGURATION

10.1.1 Installation

```
sudo apt update
sudo apt upgrade
sudo timedatectl set-timezone Asia/Phnom_Penh
sudo apt install nginx
```

10.1.2 Configuring Passthrough on port 5500, 5577, 80, and 443

In this High Availability Security Server setup with External Load Balancer, please note that the dns record for security server should be resolved to the load balancer for traffic distribution to each servers

DNS: ss.company1.com => ip_of_load_balancer

Add to the bottom of /etc/nginx/nginx.conf to include the passthrough configuration file

```
sudo vim /etc/nginx/nginx.conf
    include /etc/nginx/passthrough.conf;
```

Remove the default configuration file

```
sudo rm -rf /etc/nginx/sites-enabled/default
```

Create the passthrough configuration file

```
sudo vim /etc/nginx/passthrough.conf
    stream {
      # Log Format Configuration
      log_format basic '$remote_addr [$time_local] '
            '$protocol $status $bytes_sent $bytes_received '
            '$session_time "$upstream_addr" '
            '"$upstream_bytes_sent" "$upstream_bytes_received" "$upstream_connect_time"';
      # Log File Configuration
      access_log /var/log/nginx/ss.company1.com_access.log basic;
      error_log /var/log/nginx/ss.company1.com_error.log;

      # Upstream Configuration for port 5500, 5577, 80, and 443
      upstream camdx_5500 {
        server ip_of_ss_master:5500 max_fails=1 fail_timeout=10s;
        server ip_of_ss_slave:5500 max_fails=1 fail_timeout=10s;
      }
      upstream camdx_5577 {
        server ip_of_ss_master:5577 max_fails=1 fail_timeout=10s;
        server ip_of_ss_slave:5577 max_fails=1 fail_timeout=10s;
      }
      upstream camdx_80 {
        server ip_of_ss_master:80 max_fails=1 fail_timeout=1s;
        server ip_of_ss_slave:80 max_fails=1 fail_timeout=1s;
      }
      upstream camdx_443 {
        server ip_of_ss_master:443 max_fails=1 fail_timeout=1s;
        server ip_of_ss_slave:443 max_fails=1 fail_timeout=1s;
      }

      # Server Listener
      server {
        listen 5500;
        proxy_pass camdx_5500;
        proxy_next_upstream on;
      }
      server {
        listen 5577;
        proxy_pass camdx_5577;
        proxy_next_upstream on;
      }
      server {
        listen 80;
        proxy_pass camdx_80;
        proxy_next_upstream on;
      }
      server {
        listen 443;
        proxy_pass camdx_443;
        proxy_next_upstream on;
      }
    }
```

Test and Restart nginx

```
    sudo systemctl nginx -t
    sudo systemctl restart nginx
```

11. INSTALLING AND CONFIGURING EXTERNAL OPERATIONAL MONITORING

11.1 Minimum Requirement

- 4 GB RAM
- 100GB-250GB HDD
- Running Port **2080** (Allow access from Security Servers only)

11.2 Install a Standalone Security Server

```
sudo apt update
sudo apt upgrade
sudo timedatectl set-timezone Asia/Phnom_Penh
sudo adduser camdx-systemadmin
echo LC_ALL=en_US.UTF-8 | sudo tee -a /etc/environment
sudo locale-gen en_US.UTF-8
sudo apt-get install locales software-properties-common

echo deb [arch=all,amd64] http://repository.camdx.gov.kh/repository/camdx-release bionic main | sudo tee -a /etc/apt/sources.list

sudo apt-get update
sudo apt-get install xroad-securityserver
sudo apt-get install xroad-opmonitor

#Stop Some Services
sudo systemctl stop xroad-proxy
sudo systemctl stop xroad-jetty
sudo systemctl stop xroad-monitor

sudo systemctl disable xroad-proxy
sudo systemctl disable xroad-jetty
sudo systemctl disable xroad-monitor
```

11.3 Configure External Operational Monitoring

```
sudo vim /etc/xroad/conf.d/local.ini
    [op-monitor]
    keep-records-for-days = 30
    host = 0.0.0.0

wget http://repository.camdx.gov.kh/repository/camdx-anchors/anchors/CAMBODIA_configuration_anchor.xml
sudo mv CAMBODIA_configuration_anchor.xml configuration_anchor.xml
sudo chown –Rf xroad:xroad configuration_anchor
sudo systemctl restart xroad-opmonitor
```

11.4 Configure Master node for External Operational Monitoring

#On Security Server **Master** Node, we also need to edit a configuration file at /etc/xroad/conf.d/local.ini

```
sudo vim /etc/xroad/conf.d/local.ini
    [op-monitor]
    host = external_operation_monitoring_ip_or_domain_name
```

#Install xroad-addon-proxymonitor & xroad-addon-opmonitoring - on both **Master** and **Slave**

```
sudo apt install xroad-addon-proxymonitor
sudo apt install xroad-addon-opmonitoring
sudo systemctl restart xroad-opmonitor

sudo systemctl restart xroad-opmonitor
```

#Stop and Disable the Local Operation Monitoring Service on **Master** Node

```
sudo systemctl stop xroad-opmonitor
sudo systemctl disable xroad-opmonitor
```

#On the **Slave** Node, check at /etc/xroad/conf.d/local.ini if it is replicated, then on the **Slave** Node

```
sudo systemctl restart xroad-opmonitor
sudo systemctl stop xroad-opmonitor
sudo systemctl disable xroad-opmonitor
```

12. CONFIGURATION

Configure Security Server **Master** Node by following the "**Configuration Section**" in "Standalone Security Server Installation & Configuration Guideline".

13. REFERENCES

X-Road/ig-xlb_x-road_external_load_balancer_installation_guide.md at camdx-6.23.0 · CamDX/X-Road. (2022). Retrieved 30 May 2022, from https://github.com/CamDX/X-Road/blob/camdx-6.23.0/doc/Manuals/LoadBalancing/ig-xlb_x-road_external_load_balancer_installation_guide.md

ឧបសម្ព័ន្ធ៦៖ ឯកសារធានានូវគុណភាព និងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (Information Security Guideline)

INFORMATION SECURITY GUIDELINE

By CamDX Operator

July 2022

Contents

1. INTRODUCTION

With increasingly adoption of Cambodia Data Exchange (CamDX) for secure data exchange over public internet, the CamDX Operator has established guidelines to help members create a secured technology ecosystem. Despite the fact that data exchange via CamDX is secured, we still need to make sure that both members (provider & consumer) meet a set security requirements.

The guidelines are primarily expected to enhance the safety, security, and efficiency of members' operations, which will benefit the ecosystem as a whole.

Members may have already implemented some or many of the key areas indicated in this guideline. It is recommended to conduct the gap analysis between their current status and recommendations as laid out in this guideline and put in place a time-bound action plan to address the gap and in fulfilment of this guideline.

1.1 Terms and definitions

Asset: Any item that has value to the organization. There are many types of assets, e.g. data, hardware, software, service providers, personnel, and physical locations.

Attack: "attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset".

Availability: "property of being accessible and usable upon demand by an authorized entity".

Authenticity: "property that an entity is what it claims to be".

Confidentiality: "property that makes information available or disclosed only to authorized individuals, entities or processes".

Control: "a measure to modify risk".

Event: "occurrence or change of a particular set of circumstances".

Integrity: "property of accuracy and completeness".

Information security: "preservation of confidentiality, integrity and availability of information".

Non-repudiation: "ability to prove the occurrence of a claimed event or action and its originating entities".

Process: "set of interrelated or interacting activities which transforms inputs into outputs".

Risk (information security): An information security risk with the potential that threats will exploit the vulnerabilities of an information asset and thereby cause harm to an organization.

Risk assessment (information security): Overall process of risk identification, risk analysis and risk evaluation.

Risk treatment (information security): Process to modify risk – usually involving risk avoidance, risk sharing, risk mitigation or risk acceptance.

Threat: "potential cause of an unwanted incident, which may result in harm".

Vulnerability: "weakness of an asset or control that can be exploited by one or more threats".

2. SCOPE

This Guidline was written for and is applicable to CamDX member that rely on technological assets. Its guidelines can be easily implemented by other organizations, whatever their size or complexity.

On the basis of CS ISO/IEC 27000:2021, CS ISO/IEC 27001:2021 and CS ISO/IEC 27002:2021 content, this Guidline describes a series of practical activities that can significantly help with establishing or raising information security levels for CamDX member. This will strengthen their business and facilitate partnership opportunities within the CamDX ecosystem.

All the listed activities ensure an information security lifecycle within the organization. This includes establishing, planning, implementing, operating and improving all related processes, based on risk culture and continual improvement.

3. INFORMATION SECURITY MANAGEMENT

All information stored and processed by an organization is subject to threats of attack, error, nature disaster, etc., and is subject to vulnerabilities inherent in its use. The term information security is generally based on information asset which has a value requiring appropriate protection against the loss of availability, confidentiality and integrity. Accuracy and completeness of information must be available in a timely manner to authorized individuals in need is a catalyst for business efficiency.

Before initiating Information security management, it is essential to decide which form should be taken, the timeframe and the personnel's involvement. The earliest initiators should involve subject-matter expert as they must set up the bases for all the other activities, and top management who should be accountable for establishing the foundations of information security. The information security manager is responsible for this task while keeping the system owners and information owners updated on the progress of task development.

3.1 Roles and responsibilities

It is important to have roles and responsibilities properly assigned. When deciding to take measures to define or revise information security management within an organization.

Main roles and related responsibilities for information security management are generally described in this paragraph. Note that smaller organizations could give more than one role to the same person or outsource these roles. As a prerequisite step for applying this Guidline, CamDX member must specifically and formally assign information security roles and responsibilities according to its own structure and culture.

Top management
Having the power to delegate authority and provide resources within the organization, top management also hold great responsibility for information security governance which is important part of the overall governance. Top management usually includes the Chief Executive Officer (CEO), Chief Operating Officer (COO) or board of directors, depending on the organization's structure.

Information security committee
Working together with top management and will be responsible for auditing and monitoring activities, the information security committee should meet to deal with several issues related to information security, such as:

- security norms and procedures approval;

- risk analysis review and risk treatment plan;
- audit results and related actions;
- information security plan monitoring;
- information security goal and performance indicators;
- awareness and training sessions planning;
- emergency response.

Information security officer/manager
Any high-ranking staff member such as IT manager or Chief Technology Officer with good knowledge of information flows can hold this position. The responsibilities usually include: identifying budgets, utilizing risk/benefit models for risk estimation and treatment, drafting information security policies and procedures, and reviewing the results of monitoring activities. Information security awareness, establishment of communication channels and reporting often are the responsibility of the information security manager.

System and information owners
More structured organizations might need to identify a series of individuals to carry out tasks on a daily basis, in order to protect the information systems that they control. These are the 'system owners'. However, regardless of information systems, the requirements for data protection should be defined by the business owners since they are in charge of processes and data. These are the 'information owners'. Both categories should help the organization by ensuring that information security controls are in place and are performing adequately. Normally the owners have the modification right to whatever they own, e.g. system update, creating shortcut, etc. which could impact the information security of the organization.

Personnel
It is essential to provide proper training and education to the employees. They should understand fully the reasons behind the control environment surrounding them, so the information security could be maintained at the right level and not be compromised. Employees and contractors should be able to recognize unusual behavior and quickly raise any concerns to the information security manager, in order to minimize loss for the organization. Most of the time the potential targets of attacks are the employees and contractors so having well educated staff is considered an enhancement of overall information security environment. These staff may also be able to turn that knowledge and expertise into organizational culture.

3.2 Asset management

Before applying any information security measure, CamDX member needs to get an initial clear view of which objects really have value for them. Such objects, usually defined as assets, can be generally classified under information, which are typically intangible, and other assets which are typically tangible.

The main objective of this action is to represent the key assets that are under the control of the organization and need protection. This is especially important when identifying relations between assets and when defining responsibilities.

Inventory of assets:
Information assets shall be identified and an inventory of these assets shall be drawn up and maintained. The inventory record of each information asset should, at least, include:

- a clear and distinct identification of the asset
- relative value to the organization
- location
- security/risk classification

- asset group
- owner and
- designated custodian

Understand the connection between information and other assets:
Once all main assets are identified, establishing which ones are used for certain information is an effective way to understand what needs protection and, later on, how much protection it needs.

The right level of access controls should be applied to each information asset. Remember that the asset map must be constantly updated along with its access controls to build and maintain a consistent perspective of the security requirements. The additional controls to protect the information assets should include, but not limited to:

- service level management
- vendor management
- capacity management and
- configuration management

3.3 Information security risk management

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, CamDX member should understand the likelihood that an event will occur and the potential resulting impacts. With this information, member can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

With an understanding of risk tolerance, member can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers member the ability to quantify and communicate adjustments to their cybersecurity programs. CamDX member may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

Some of the world leading cyber security risk assessment frameworks have evolved based on five key principles: identify, detect, protect, respond and recover. These Functions are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

- **Identify** – Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities. The activities in the Identify principle are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

- **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect principle supports the ability to limit or contain the impact of a potential cyber security event.

- **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect principle enables timely discovery of cybersecurity events.

- **Respond**: Develop and implement the appropriate activities to take action regarding a detected cyber security event. The Respond principle supports the ability to contain the impact of a potential cyber security event and

- **Recover**: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. The Recover principle supports timely recovery to normal operations to reduce the impact from a cyber security event.

4. INFORMATION SECURITY POLICIES

CamDX member needs to put in place an approved Information Security Policy and must identify and implement appropriate information security management measures or practices keeping in view their business needs. Given the critical role of technology as part of its business, member needs to subject them to suitable controls across their lifecycle. The specified policy should include, but not be limited to the following:

Information security must uphold confidentiality, integrity and availability (known as the CIA triad) as the core principles.

- **Confidentiality**: "property that information is not made available or disclosed to unauthorized individuals, entities, or processes".
- **Integrity**: "property of accuracy and completeness".
- **Availability**: "property of being accessible and usable on demand by an authorized entity"

Other principles such as authenticity, non-repudiation, identification, authorization, accountability and auditability are also becoming key considerations for practical security implementations.

- **Authenticity**: "property that an entity is what it claims to be".
- **Non-repudiation**: "ability to prove the occurrence of a claimed event or action and its originating entities".
- **Identification**: identification is the process by which a subject admits an identity and accountability is initiated.
- **Authentication**: "provision of assurance that a claimed characteristic of an entity is correct".
- **Authorization**: "the right or a permission that is granted to a system entity to access a system resource".
- **Accountability**: "the property that ensures that the actions of an entity may be traced uniquely to the entity".

4.1 Access control

Objective: To limit access to information and information processing facilities.

Control
An access control policy should be established, documented and reviewed based on business and information security requirements.

Implementation guidance
Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.

Access controls are both logical and physical and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take into account of the following:

- security requirements of business applications;
- policies for information dissemination and authorization;
- consistency between the access rights and information classification policies of systems and networks;
- relevant legislation and any contractual obligations regarding limitation of access to data or services;
- management of access rights in a distributed and networked environment which recognizes all types of connections available;
- segregation of access control roles, e.g. access request, access authorization, access administration;
- requirements for formal authorization of access requests;
- requirements for periodic review of access rights;
- removal of access rights;
- archiving of records of all significant events concerning the use and management of user identities and secret authentication information;
- roles with privileged access.

Other information
Care should be taken when specifying access control rules to consider:

- establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";
- changes in information labels that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
- changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
- rules which require specific approval before enactment and those which do not.

It is recommended to consider role based access control, also known as a non-discretionary access control, which is an approach used to link access rights with business roles. Additionally, two of the frequent principles for the access control policy are:

- Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile);
- Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

4.2 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

4.2.1 Network controls

Control
Networks should be managed and controlled to protect information in systems and applications.

Implementation guidance
Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered:

- responsibilities and procedures for the management of networking equipment should be established;
- operational responsibility for networks should be separated from computer operations where appropriate;
- special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications; special controls may also be required to maintain the availability of the network services and computers connected;
- appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security;
- management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;
- systems on the network should be authenticated;
- systems connection to the network should be restricted.

4.2.2 Security of network services

Control
Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Implementation guidance
The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

- technology applied for security of network services, such as authentication, encryption and network connection controls;
- technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
- procedures for the network service usage to restrict access to network services or applications, where necessary.

4.2.3 Segregation in networks

Control
Groups of information services, users and information systems should be segregated on networks.

Implementation guidance
One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop

domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks (e.g. virtual private networking).

The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy, access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable
gateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy before granting access to internal systems.

The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organization’s internal network when properly implemented.

4.3 Mobile devices and remote access

Objective: To ensure the security of teleworking and use of mobile devices.

4.3.1 Mobile device policy

Control
A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Implementation guidance
When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

The mobile device policy should consider:

- registration of mobile devices;
- requirements for physical protection;
- restriction of software installation;
- requirements for mobile device software versions and for applying patches;
- restriction of connection to information services; access controls;
- cryptographic techniques;
- malware protection;
- remote disabling, erasure or lockout;
- backups;
- usage of web services and web apps.

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques and enforcing use of secret authentication information.

Mobile devices should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of mobile devices. Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

Training should be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented.

Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

- separation of private and business use of the devices, including using software to support such separation and protect business data on a private device;
- providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.

Other information

Mobile device wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are:

- some wireless security protocols are immature and have known weaknesses;
- information stored on mobile devices may not be backed-up because of limited network bandwidth or because mobile devices may not be connected at the times when backups are scheduled.

Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organization's premises.

4.3.2 Remote access

Control

A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

Implementation guidance

Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

- the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;
- the proposed physical teleworking environment;
- the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will

be accessed and passed over the communication link and the sensitivity of the internal system;

- the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;
- the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;
- the use of home networks and requirements or restrictions on the configuration of wireless network services;
- policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;
- access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;
- software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users;
- malware protection and firewall requirements.

The guidelines and arrangements to be considered should include:

- the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed;
- a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;
- the provision of suitable communication equipment, including methods for securing remote access;
- physical security;
- rules and guidance on family and visitor access to equipment and information;
- the provision of hardware and software support and maintenance;
- the provision of insurance;
- the procedures for backup and business continuity;
- audit and security monitoring;
- revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

Other information

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible workplace”, “remote work” and “virtual work” environments.

4.4 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

Control

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Implementation guidance

A current and complete inventory of assets is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

Appropriate and timely action should be taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

- the organization should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;
- information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list); these information resources should be updated based on changes in the inventory or when other new or useful resources are found;
- a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;
- once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls;
- depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures;
- if a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);
- patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:
  - turning off services or capabilities related to the vulnerability;
  - adapting or adding access controls, e.g. firewalls, at network borders;
  - increased monitoring to detect actual attacks;
  - raising awareness of the vulnerability;
- an audit log should be kept for all procedures undertaken;
- the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;
- systems at high risk should be addressed first;
- an effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur;
- define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

Other information

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures. Vendors are often under significant pressure to release patches as soon as possible. Therefore, there is a possibility that a patch does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling a patch cannot be easily achieved once the patch has been applied. If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users.

4.5 Physical and environmental security

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. Conceptually, those physical security risks are mitigated through zone-oriented implementations. Zones are physical areas with differing physical security requirements. The security requirements of each zone are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone.

The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but is not limited to, threats like dust, electrical supply interference, electromagnetic radiation, explosives, fire, smoke, theft/destruction, vibration/earthquake, water, criminals, terrorism, political issues (e.g. strikes, disruptions) and other threats based on the entity's unique geographical location, building configuration, neighboring environment/ entities, etc.

These security controls are applicable to locations where critical information assets are kept, such as the data center, disaster recovery site, server room, etc.

Consideration Points

- Environmental controls:
  - It is important to secure location of critical assets to protect them from natural and man-made threats
  - Access to sensitive areas like data centers should be restricted including detailed procedures for handling access by internal staff, contracters and visitors and
  - Monitoring mechanisms for the detection of compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunications, servers), access log reviews, etc.
- Perimeters of a building or site containing information processing facilities should be physically secure (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.
- A manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only.
- Physical barriers should, wherever applicable, be built to prevent unauthorized physical access and environmental contamination.
- All fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner.
- Suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms.
- The date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions

on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means.

- Access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card.
- A physical log book or electronic audit trail of all access should be securely maintained and monitored.
- All employees, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.
- External party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorized and monitored.
- Access rights to secure areas should be regularly reviewed and updated, and revoked when necessary.
- Where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities.
- Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
    - Procedures for working in secure areas should be designed and applied.
    - Personnel should only be aware of the existence of, or activities within, a secure area on a need to-know basis.
    - Unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities.
    - Vacant secure areas should be physically locked and periodically reviewed and
    - Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.
- There should be secure storage of media. Controls could include physical and environmental controls such as fire and flood protection, limiting access by means of physical locks, keypad, passwords, biometrics, etc., labelling, and logged access. Management should establish access controls to limit access to media, while ensuring that all employees have authorization to access the minimum data required to perform their responsibilities.

4.6 System and Application Security Controls

There are different types of applications like the network operating systems, databases, enterprise resource management systems, customer relationship management systems, all used for different business purposes. Users usually access several different types of systems throughout their daily tasks making controlling access and providing the necessary level of protection on different data types difficult and full of obstacles. This complexity may result in unforeseen and unidentified holes in the protection of the entire infrastructure including overlapping and contradictory controls, and policy and regulatory noncompliance. There are commonly known information systems vulnerability associated with application software, whether the software is in-house developed or acquired from an external source. Threat actors can potentially use many different paths through the application to cause damage to the business; thus it is essential to have strong application controls embedded in an enterprise.

Consideration Points

- Owner should be assigned to each application, which will usually be the concerned business function that uses the application.

- It is recommended to test all application systems in the development environment before going live production.
- All critical applications should conduct source code review; at least, this should be after every major update.
- The organization should exercise due diligence in ensuring its applications have appropriate security controls, taking into consideration the type of processes and complexity of services these applications provide in order to ensure that there is a high degree of system and data integrity.
- Recovery measures, user access and data protection controls, at the minimum, should be implemented for such applications.
- All application systems should have audit trails including the clear allocation of responsibilities in this regard.
- There should be documented standards/procedures for administering the application, which are approved by the application owner and kept up-to-date.
- There should be measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties.
- Robust System Security Testing, in respect of critical systems, needs to incorporate, among other things, specifications relating to information leakage, business logic, authentication, authorization, input data validation, exception/error handling, session management, cryptography and detailed logging, as relevant. This needs to be carried out at least every year and
- Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy. The following should be considered in order to support access restriction requirements:
  - Providing menus to control access to application system functions
  - Controlling which data can be accessed by a particular user
  - Controlling the access rights of users, e.g. read, write, delete and execute
  - Controlling the access rights of other applications
  - Limiting the information contained in outputs and
  - Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems

4.7 Operations security

4.7.1 Documented operating procedures

Control
Operating procedures should be documented and made available to all users who need them.

Implementation guidance
Documented procedures should be prepared for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management and safety.

The operating procedures should specify the operational instructions, including:

- the installation and configuration of systems;
- processing and handling of information both automated and manual;
- backup;
- scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

- instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
- support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;
- special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;
- system restart and recovery procedures for use in the event of system failure;
- the management of audit-trail and system log information;
- monitoring procedures.

Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

4.7.2 Change management

Control
Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

Implementation guidance
In particular, the following items should be considered:

- identification and recording of significant changes;
- planning and testing of changes;
- assessment of the potential impacts, including information security impacts, of such changes;
- formal approval procedure for proposed changes;
- verification that information security requirements have been met;
- communication of change details to all relevant persons;
- fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events;
- provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident.

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.

Other information
Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications.

4.7.3 Separation of development, testing and operational environments

Control
Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.
Implementation guidance

The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

- rules for the transfer of software from development to operational status should be defined and documented;
- development and operational software should run on different systems or computer processors and in different domains or directories;
- changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems;
- other than in exceptional circumstances, testing should not be done on operational systems;
- compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;
- users should use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error;
- sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system

Other information
Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the operational environment.

Where development and testing personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud or introduce untested or malicious code, which can cause serious operational problems.

Development and testing personnel also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, testing and operational environments is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data

4.8 Information security incident management

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

4.8.1 Responsibilities and procedures

Control
Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Implementation guidance
The following guidelines for management responsibilities and procedures with regard to information security incident management should be considered:

- management responsibilities should be established to ensure that the following procedures are developed and communicated adequately within the organization:
    - procedures for incident response planning and preparation;

    - procedures for monitoring, detecting, analyzing and reporting of information security events and incidents;
    - procedures for logging incident management activities;
    - procedures for handling of forensic evidence;
    - procedures for assessment of and decision on information security events and assessment of information security weaknesses;
    - procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations;
- procedures established should ensure that:
    - competent personnel handle the issues related to information security incidents within the organization;
    - a point of contact for security incidents' detection and reporting is implemented;
    - appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained;
- reporting procedures should include:
    - preparing information security event reporting forms to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event;
    - the procedure to be undertaken in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact and taking only coordinated actions;
    - reference to an established formal disciplinary process for dealing with employees who commit security breaches;
    - suitable feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

Other information
Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.

4.8.2 Reporting information security events

Control
Information security events should be reported through appropriate management channels as quickly as possible.

Implementation guidance
All employees and contractors should be made aware of their responsibility to report information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported.

Situations to be considered for information security event reporting include:

- ineffective security control;
- breach of information integrity, confidentiality or availability expectations;
- human errors;

- non-compliances with policies or guidelines;
- breaches of physical security arrangements;
- uncontrolled system changes;
- malfunctions of software or hardware;
- access violations.

Other information
Malfunctions or other anomalous system behavior may be an indicator of a security attack or actual security breach and should therefore always be reported as an information security event.

4.8.3 Reporting information security weaknesses

Control
Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

Implementation guidance
All employees and contractors should report these matters to the point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible and available as possible.

Other information
Employees and contractors should be advised not to attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

4.8.4 Assessment of and decision on information security events

Control
Information security events should be assessed and it should be decided if they are to be classified as information security incidents.

Implementation guidance
The point of contact should assess each information security event using the agreed information security event and incident classification scale and decide whether the event should be classified as an information security incident. Classification and prioritization of incidents can help to identify the impact and extent of an incident.

In cases where the organization has an information security incident response team (ISIRT), the assessment and decision can be forwarded to the ISIRT for confirmation or reassessment.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

4.8.5 Response to information security incidents

Control
Information security incidents should be responded to in accordance with the documented procedures.

Implementation guidance

Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organization or external parties.

The response should include the following:

- collecting evidence as soon as possible after the occurrence;
- conducting information security forensics analysis, as required;
- escalation, as required;
- ensuring that all involved response activities are properly logged for later analysis;
- communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;
- dealing with information security weakness(es) found to cause or contribute to the incident;
- once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis should take place, as necessary, to identify the source of the incident.

Other information
The first goal of incident response is to resume 'normal security level' and then initiate the necessary recovery

4.8.6 Learning from information security incidents

Control
Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Implementation guidance
There should be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

Other information
The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process. With due care of confidentiality aspects, anecdotes from actual information security incidents can be used in user awareness training as examples of what could happen, how to respond to such incidents and how to avoid them in the future.

4.8.7 Collection of evidence

Control
The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Implementation guidance
Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.

In general, these procedures for evidence should provide processes of identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off. The procedures should take account of:

- chain of custody;
- safety of evidence;

- safety of personnel;
- roles and responsibilities of personnel involved;
- competency of personnel;
- documentation;
- briefing.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Forensic evidence may transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as forensic evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.

Other information
Identification is the process involving the search for, recognition and documentation of potential evidence. Collection is the process of gathering the physical items that can contain potential evidence. Acquisition is the process of creating a copy of data within a defined set. Preservation is the process to maintain and safeguard the integrity and original condition of the potential evidence.

When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.

4.9 Information security aspects of business continuity management

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

4.9.1 Planning information security continuity

Control
The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

Implementation guidance
An organization should determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process. Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

Other information
In order to reduce the time and effort of an 'additional' business impact analysis for information security, it is recommended to capture information security aspects within the normal business continuity management or disaster recovery management business impact analysis. This implies

that the information security continuity requirements are explicitly formulated in the business continuity management or disaster recovery management processes.

4.9.2 Implementing information security continuity

Control
The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Implementation guidance
An organization should ensure that:

- an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
- incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;
- documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives

According to the information security continuity requirements, the organization should establish, document, implement and maintain:

- information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
- processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;
- compensating controls for information security controls that cannot be maintained during an adverse situation.

Other information
Within the context of business continuity or disaster recovery, specific processes and procedures may have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them should be protected. Therefore an organization should involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures.

Information security controls that have been implemented should continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls should be established, implemented and maintained to maintain an acceptable level of information security.

4.9.3 Verify, review and evaluate information security continuity

Control
The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Implementation guidance
Organizational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such

cases, the continuity of processes, procedures and controls for information security should be reviewed against these changed requirements.

Organizations should verify their information security management continuity by:

- exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;
- exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives;
- reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

Other information

The verification of information security continuity controls is different from general information security testing and verification and should be performed outside the testing of changes. If possible, it is preferable to integrate verification of information security continuity controls with the organization's business continuity or disaster recovery tests.

4.10 Audit trails

CamDX member needs to ensure that audit trails exist for IT assets satisfying the business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. This could include, as applicable, various areas like transaction with financial consequences, modifications in sensitive master data, accessing or copying of sensitive data/information; and granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.

Audit trails should be secured to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails should be in line with business, regulatory and legal requirements.

Audit and security logs are useful information which facilitates investigations and trouble shooting.

Consideration Points

- Ensure that records of user access are uniquely identified and logged for audit and review purposes.
- Have accountability and identification of unauthorized access is documented.
- Enable audit logging of system activities performed by privileged users.
- Protect against unauthorized changes to log information by using appropriate logging facility. The operational control should include protection from:
  - alterations to the message types that are recorded
  - log files being edited or deleted and
  - storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.
- Ensure that Network Time Protocol (NTP) server is used to time sync all internal devices.
- Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security.
- Ensure event logs include, when relevant:
  - User IDs

    - System activities
    - Dates, time and details of key events, e.g. log-on and log-off
    - Device identity or location if possible and system identifier
    - Records of successful and rejected system access attempts
    - Records of successful and rejected data and other resource access attempts
    - Changes to system configuration
    - Use of privileges
    - Use of system utilities and applications
    - Files accessed and the kind of access
    - Network addresses and protocols
    - Alarms raised by the access control system and
    - Records of transactions executed by users in applications and online customer transaction
- Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

5. REFERENCES

CS ISO/IEC 27000:2021 (IDT/ED 2018)

CS ISO/IEC 27001:2021 (IDT/ED 2013)

CS ISO/IEC 27002:2021 (IDT/ED 2013)

Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity version 1.1.

(2022). Retrieved 21 July 2022, from https://www.nbc.org.kh/download_files/publication/itguideline_eng/NBC-Risk-Management-Guidelines-July%202019.pdf

(2022). Retrieved 21 July 2022, from https://sbs-sme.eu/sites/default/files/publications/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min%20%281%29.pdf

(2022). Retrieved 21 July 2022, from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf

ឧបសម្ព័ន្ធ៧៖ បញ្ជីត្រួតពិនិត្យគុណភាព និងសុវត្ថិភាពប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន (Information Security Guideline Checklist)

Information Security Guideline

Checklist

I, the undersigned, acting on behalf of the organization, hereby declare that the information provided below is true, complete and correct. I also understand that in the event of my information being found false or incorrect at any stage, the CamDX membership application for the organization shall be liable to cancellation or termination without notice or any compensation in lieu thereof.

Name of the organization: ____

Name and position of the representative: ____

Signature ____________________________________Date____

The notion for compliance to the guideline, to fill in the “Confirm” section, is as below:

- 0 : non-compliant (the organization fails to comply with section)
- 1 : partially compliant (some aspects or parts of the section are met while others are not)
- 2 : substantially compliant (to a large extent in accordance with the section)
- 3 : fully compliant (entirely in accordance with the section, which is implemented in an effective manner)

It is recommended to also provide information in addition to the confirmation status in the “Others” section.

Information Security Guideline Checklist				
Reference	**Confirmation area, objective and question**		**Results**	
Checklist	**Guideline Section**	**Checklist Question**	**Confirm**	**Others**
1	**3. Information security management**			
1.1	**3.1 Roles and responsibilities**	Whether roles and responsibilities are defined and assigned.		
1.2	**3.2 Asset management**	Whether the assets, to be protected, are identified.		
1.3	**3.3 Information security risk management**	Whether risks to the organization’s information and information processing facility, from a process involving external party access, is identified and appropriate control measures implemented before granting access.		

Information Security Guideline Checklist				
Reference	**Confirmation area, objective and question**		**Results**	
Checklist	**Guideline Section**	**Checklist Question**	**Confirm**	**Others**
2	**4. Information security policies**			
2.1	**4.1 Access control**	Whether an access control policy is developed and reviewed based on the business and security requirements.		
2.2	**4.2 Network security management**			
2.2.1	**4.2.1 Network controls**	Whether the network is adequately managed and controlled, to protect from threats, and to maintain security for the systems and applications using the network, including the information in transit.		
2.2.2	**4.2.2 Security of network services**	Whether security features, service levels and management requirements, of all network services, are identified and included in any network services agreement.		
2.2.3	**4.2.3 Segregation in networks**	Whether groups of information services, users and information systems are segregated on networks. Whether the network (where business partner's and/ or third parties need access to information system) is segregated using perimeter security mechanisms such as firewalls. Whether consideration is made to segregation of wireless networks from internal and private networks.		

Information Security Guideline Checklist

Reference	**Confirmation area, objective and question**		**Results**	
Checklist	**Guideline Section**	**Checklist Question**	**Confirm**	**Others**
2.3	**4.3 Mobile devices and remote access**			
2.3.1	**4.3.1 Mobile device policy**	Whether the risks of working with mobile devices in unprotected environments are taken into account.		
2.3.2	**4.3.2 Remote access**	Whether a policy and supporting security measures are implemented to protect information accessed, processed or stored at teleworking sites.		
2.4	**4.4 Technical vulnerability management**	Whether timely information about technical vulnerabilities of information systems being used is obtained. Whether the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to mitigate the associated risk.		
2.5	**4.5 Physical and environmental security**	Whether a physical border security facility has been implemented to protect the information processing service. Whether entry controls are in place to allow only authorized personnel into various areas within the organization. Whether the rooms, which have the information processing service, are locked or have lockable cabinets or safes.		

Information Security Guideline Checklist				
Reference	**Confirmation area, objective and question**		**Results**	
Checklist	**Guideline Section**	**Checklist Question**	**Confirm**	**Others**
2.6	**4.6 System and application security controls**	Whether access to information and application system functions by users and support personnel is restricted in accordance with the defined access control policy.		
2.7	**4.7 Operations security**			
2.7.1	**4.7.1 Documented operating procedures**	Whether the operating procedure is documented, maintained and available to all users who need it.		
2.7.2	**4.7.2 Change management**	Whether all changes to information processing facilities and systems are controlled.		
2.7.3	**4.7.3 Separation of development, testing and operational environments**	Whether the development and testing environment are isolated from operational environment. For example, development and production software should be run on different computers. Where necessary, development and production networks should be kept separate from each other.		

<table>
<tr><th colspan="5">Information Security Guideline Checklist</th></tr>
<tr><th>Reference</th><th colspan="2">Confirmation area, objective and question</th><th colspan="2">Results</th></tr>
<tr><th>Checklist</th><th>Guideline Section</th><th>Checklist Question</th><th>Confirm</th><th>Others</th></tr>
<tr><td>2.8</td><td colspan="4"><b>4.8 Information security incident management</b></td></tr>
<tr><td>2.8.1</td><td><b>4.8.1 Responsibilities and procedures</b></td><td>Whether management responsibilities and procedures were established to ensure quick, effective and orderly response to information security incidents.
Whether monitoring of systems, alerts and vulnerabilities are used to detect information security incidents.</td><td></td><td></td></tr>
<tr><td>2.8.2</td><td><b>4.8.2 Reporting information security events</b></td><td>Whether information security events are reported through appropriate management channels as quickly as possible.
Whether formal information security event reporting procedure, Incident response and escalation procedure are developed and implemented.</td><td></td><td></td></tr>
<tr><td>2.8.3</td><td><b>4.8.3 Reporting information security weaknesses</b></td><td>Whether there exists a procedure that ensures all employees of information systems and services are required to note and report any observed or suspected security weakness in the system or services.</td><td></td><td></td></tr>
<tr><td>2.8.4</td><td><b>4.8.4 Assessment of and decision on information security events</b></td><td>Whether the Information security events are assessed and decided if they are to be classified as information security incidents.</td><td></td><td></td></tr>
</table>

Information Security Guideline Checklist				
Reference	Confirmation area, objective and question		Results	
Checklist	Guideline Section	Checklist Question	Confirm	Others
2.8.5	**4.8.5 Response to information security incidents**	Whether the information security incidents are responded to by a nominated point of contact and other relevant persons of the organization or external parties.		
2.8.6	**4.8.6 Learning from information security incidents**	Whether there is a mechanism in place to identify and quantify the type, volume and costs of information security incidents. Whether the information gained from the evaluation of the past information security incidents are used to identify recurring or high impact incidents.		
2.8.7	**4.8.7 Collection of evidence**	Whether evidence relating to the incident are collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Whether internal procedures are developed and followed when collecting and presenting evidence for the purpose of disciplinary action within the organization.		

Information Security Guideline Checklist				
Reference	**Confirmation area, objective and question**		**Results**	
Checklist	**Guideline Section**	**Checklist Question**	**Confirm**	**Others**
2.9	**4.9 Information security aspects of business continuity management**			
2.9.1	**4.9.1 Planning information security continuity**	Whether plans were developed to maintain and restore business operations, ensure availability of information within the required level in the required time frame following an interruption or failure to business processes.		
2.9.2	**4.9.2 Implementing information security continuity**	Whether the plan considers identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedure, documentation of procedure and regular testing.		
2.9.3	**4.9.3 Verify, review and evaluate information security continuity**	Whether Business continuity plans are tested regularly to ensure that they are up to date and effective. Whether business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when plan is evoked.		

Information Security Guideline Checklist				
Reference	**Confirmation area, objective and question**		**Results**	
Checklist	**Guideline Section**	**Checklist Question**	**Confirm**	**Others**
2.10	**4.10 Audit trails**	Whether there exist the audit trails for IT assets satisfying the business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution.		

ឧបសម្ព័ន្ធ៨៖ CamDigiKey KYC Verification API

CAMDIGIKEY KYC VERIFICATION API

Organization Level's Open API
By CamDX Operator

Release V2.0.0 – July 2022

DOCUMENT VERSION HISTORY

RELEASE NO	AUTHOR	DATE	BRIEF SUMMARY OF CHANGES
2.0.0	**CamDX Operator**	**JULY 2022**	❖ **VERIFY USER INFO** ❖ **VERIFY USER INFO AND USER FACE** ❖ **VERIFY USER INFO, ID CARD AND USER FACE** ❖ **VERIFY USER INFO, ID CARD IMAGE, AND LIVENESS** ❖ **KHMER ID CARD OCR**

Contents

1. INTRODUCTION

CamDigiKey is a E-KYC service provider focusing on convenience and security for users. Basically, users need to register themselves to the application by providing their faces and identity documents such as ID card or passport. Once the user's account is approved, they can use CamDigiKey mobile application to login to any CamDigiKey partner's portals.

For organization or institution, CamDigiKey provides open KYC verification APIs which enable fast user on board on the organization or institution's platform. The open KYC verification APIs consist of checking user info and face against data from Ministry of Interior (MOI) and verifying user liveness to ensure user is a real human.

This document will focus on integration with CamDigiKey as authentication/authorization and the usage of open KYC verification APIs via Cambodia Data eXchange (CamDX).

2. OPEN KYC VERIFICATION APIS

Open KYC verification APIs are available over CamDX which is an interoperability platform of Cambodia government. The KYC verification APIs consist of 5 APIs:

Request Based URL:
http(s)://{REQUESTER_SS_MEMBER_ADDR}/r1/CAMBODIA/GOV/{CAMDIGIKEY_MEMBER_CODE}/CAMDIGIKEY_KYC
Request Header:
X-Road-Client: CAMBODIA/GOV/{REQUESTER_SS_MEMBER_CODE}/{REQUESTER_SS_SUBSYSTEM_CODE}

Environment	CAMDIGIKEY_MEMBER_CODE
DEVELOPMENT	CAMDX-20201222
PRODUCTION	CAMDX-00003

Example:

DEVELOPMENT:

http(s)://dev.ss.camdx.gov.kh:8443/r1/CAMBODIA/GOV/CAMDX-20201222/CAMDIGIKEY_KYC

PRODUCTION:

http(s)://ss.camdx.gov.kh/r1/CAMBODIA/GOV/CAMDX-000003/CAMDIGIKEY_KYC

2.1 Verify User Info

<table>
<tr><th>No</th><th colspan="2">Verification between submitted information with MOI information</th></tr>
<tr><td rowspan="5">1</td><td><b>API Endpoint</b></td><td>http(s)://{request_base_url}/info</td></tr>
<tr><td><b>Method</b></td><td>POST</td></tr>
<tr><td><b>Format</b></td><td>JSON</td></tr>
<tr><td><b>Request params</b></td><td>

```
{
    "idNumber" : "id_number",
    "firstNameKh" : "first_name_kh",
    "lastNameKh" : "last_name_kh",
    "firstNameEn" : "first_name_en",
    "lastNameEn" : "last_name_en",
    "gender" : "M_or_F",
    "dob" : "yyyy-MM-dd",
    "issuedDate" : "yyyy-MM-dd",
    "expiredDate" : "yyyy-MM-dd"
}
```

</td></tr>
<tr><td><b>Response payload</b></td><td>

```
{
    "error": 0,
    "message": "Successfully",
    "data": {
        "idNumber": "id_number",
        "score": 1, #Range [0,1]
        "incorrectFields": [requested_fields_or_empty]
    }
}
```

</td></tr>
</table>

2.2 Verify User Info and User Face

No	Verification between submitted user information include face image with MOI information	
2	**API Endpoint**	http(s)://{request_base_url}/info-face
	Method	POST
	Format	JSON

	Request params	{
		    "userInfo" : {
		        "idNumber" : "id_number",
		        "firstNameKh" : "first_name_kh",
		        "lastNameKh" : "last_name_kh",
		        "firstNameEn" : "first_name_en",
		        "lastNameEn" : "last_name_en",
		        "gender" : "M_or_F",
		        "dob" : "yyyy-MM-dd",
		        "issuedDate" : "yyyy-MM-dd",
		        "expiredDate" : "yyyy-MM-dd"
		    },
		    "faceImg" : "base_64_content"
		}

	Response payload	{
		    "error": 0,
		    "message": "Successfully",
		    "data": {
		        "userInfo": {
		            "idNumber": "id-card-number",
		            "score": 1, #Range [0,1]
		            "incorrectFields": []
		        },
		        "faceMoiScore": 0.9792682 # Range [0,1]
		    }
		}

2.3 Verify User Info, ID Card and User Face

No	- Verification with submitted document, face verification with retrieved image from MOI - Verification of submitted information with MOI information	
3	**API Endpoint**	http(s)://{request_base_url}/info-face-idcard
	Method	POST
	Format	JSON

	Request params	{
		"userInfo" : {
		"idNumber" : "id_number",
		"firstNameKh" : "first_name_kh",
		"lastNameKh" : "last_name_kh",
		"firstNameEn" : "first_name_en",
		"lastNameEn" : "last_name_en",
		"gender" : "M_or_F",
		"dob" : "yyyy-MM-dd",
		"issuedDate" : "yyyy-MM-dd",
		"expiredDate" : "yyyy-MM-dd"
		},
		"faceImg" : "base_64_content",
		"idImage" : "base_64_content"
		}

	Response payload	{
		"error": 0,
		"message": "Successfully",
		"data": {
		"userInfo": {
		"idNumber": "id_number",
		"score": 1, #Range[0,1]
		"incorrectFields": []
		},
		"faceDocumentScore": 0.9457877, #Range[0,1]
		"faceMoiScore": 0.9792682 #Range[0,1]
		}
		}

2.4 Verify User Info, ID Card Image, and Liveness

No	- Liveness verification check, face verification with submitted document, face verification with retrieved image from MOI - Verification of submitted information with MOI information	
3	**API Endpoint**	http(s)://{request_base_url}/info-idcard-liveness
	Method	POST
	Format	JSON

	Request params	`{`
		`#1: turn face to the left, 2: turn face to the right, 3: nod the head`
		`    "actions":["2","1","3"],`
		`    "userInfo" : {`
		`        "idNumber" : "id_number",`
		`        "firstNameKh" : "first_name_kh",`
		`        "lastNameKh" : "last_name_kh",`
		`        "firstNameEn" : "first_name_en",`
		`        "lastNameEn" : "last_name_en",`
		`        "gender" : "M_or_F",`
		`        "dob" : "yyyy-MM-dd",`
		`        "issuedDate" : "yyyy-MM-dd",`
		`        "expiredDate" : "yyyy-MM-dd"`
		`    },`
		`    "idImage" : "base_64_content",`
		`    "liveness" : "base_64_content"`
		`}`

	Response payload	`{`
		`    "error": 0,`
		`    "message": "Successfully",`
		`    "data": {`
		`        "userInfo": {`
		`            "idNumber": "010682723",`
		`            "score": 1,`
		`            "incorrectFields": []`
		`        },`
		`        "livenessScore": 0.9248705,`
		`        "faceDocumentScore": 0.94440883,`
		`        "faceMoiScore": 0.9769943`
		`    }`
		`}`

2.5 Khmer ID Card OCR

No	OCR extracts user's information from submitted identification image	
3	**API Endpoint**	http(s)://{request_base_url}/ocr-idcard
	Method	POST
	Format	JSON

	Request params	{
		"idImage" : "base_64_content"
		}

	Response payload	{
		"error": 0,
		"message": "Successfully",
		"data": {
		"idNumber" : "id_number",
		"firstNameKh" : "first_name_kh",
		"lastNameKh" : "last_name_kh",
		"firstNameEn" : "first_name_en",
		"lastNameEn" : "last_name_en",
		"gender" : "M_or_F",
		"dob" : "yyyy-MM-dd",
		"issuedDate" : "yyyy-MM-dd",
		"expiredDate" : "yyyy-MM-dd"
		"MRZ1" : "String",
		"MRZ2" : "String",
		"MRZ3" : "String",
		}
		}

3. CONTACT US

- Email: camdx-info@techostartup.center
- Address: Floor 11, Business Development Center, OCIC Blvd, Sangkat Chroy Changvar, Khan Chroy Changvar, Phnom Penh, Cambodia