Landis+Gyr AG
Theilerstrasse 1
Postfach 260
6301 Zug
Switzerland

Zug, August 27, 2015 **| PUBLIC**

GRIDSTREAM PKI-POLICY

EMEA-IS-POL005-PKI_Gridstream

Department	Information Security
Version	1.7
Classification	PUBLIC
Printed Date	2020-06-11
Author	Wim Ton
Approved by	Information Security Manager EMEA
Approval Date	2015-10-14
Status	APPROVED
Reference-ID	EMEA-IS-POL005
Name	PKI_Gridstream

The electronic file is the official version and supersedes any printed version.

Table of Contents

1 | Version Control

Version	Date	Author	Details
0.1	05.04.2012	Wim Ton	Initial version
0.2	18.03.2013	Wim Ton	Changed DC certificates after feedback from DC team.
1.0	03.07.2013	Wim Ton	
1.1	30.07.2013	Wim Ton	Added externally signed sub CAs
1.2	22.11.2013	Wim Ton	Major overhaul; layout, names, root CA processes, feedback from Pauli.
1.3	12.11.2013	Wim Ton	Changes after feedback from Claudia.
1.4	10.02.2014	Wim Ton	Update DC profiles
1.5	25.03.2014	Wim Ton	Update with comments from Th. Mosel and C Schromm: moved non Gridstream CPS to separate documents.
1.6	2016-03-21	Thomas Mosel	Corrected Version Number and security role for EMEA
1.7	2016-06-07	Wim Ton	Corrected link in 2 |

2 | Related Documents

Document Name	**Document Location**
Common PKI Spezifikation V2.0	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
RFC 5280 PKIX Certificate and CRL Profile	http://www.ietf.org/rfc/rfc5280.txt
BSI TR-03109-4 Smart Metering PKI, Public Key Infrastruktur für Smart Meter Gateways -	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109-SMG_PKI.pdf
Baseline Requirements V1	https://www.cabforum.org/Baseline_Requirements_V1.pdf
Trust Service Principles and Criteria for Certification Authorities Version 2.0 March 2011	http://www.webtrust.org/homepage-documents/item54279.pdf

Landis + Gyr is not responsible for the content of the referenced documents.

3 | Terms and Abbreviations

Term/ Abbriviation	Defintion
ISMS	Information Security Management System
AIM	L+G automatic meter reading system
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CA	Certification Authority
Certificate	Name and public key, signed by a certification authority
CMS	Cryptographic Message Syntax
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practice Statement
CRMF	Certificate Request Message Format
CSR	Certificate Signing Request
DC	Data Concentrator
DN	Distinguished Name
DNS	Domain Name Service
HAN	Home Area Network
HSM	Hardware Security Module
LAN	Local Area Network
ODEP	Open Data Exchange Protocol, a specific protocol for metering data.
OTA	Over The Air, remote key or firmware update.
OU	Organisational Unit (part of a X509 name)
Out of band	Over a different communication channel, like mail/phone, email/fax.
P2P	Point to Point communication (GPRS etc.)
PED	PIN Entry Device

PLC	Power Line Communication
PKI	Public Key Infrastructure
PoC	Proof of Concept
RA	Registration Authority
SIM	Subscriber Identity Module
SM-GW	Smart Meter Gateway
TLS	Transport Layer Security (successor of SSL)
TR	Technical Guideline, German BSI standard.
WAN	Wide Area Network
X509	Standard for the contents of a certificate.

1. Security Policy

1.1. Introduction

Landis + Gyr will use a PKI to simplify the management of the keys for smart metering equipment. The use of a PKI provides a single entity where every device or partner can verify the authenticity of keys and software.

The PKI is not completely 'public'; the issued certificates will be mainly used by systems and devices sold to our customers.

Landis + Gyr runs an own root CA for the following reasons:

- Use policies that are more suited to the semi closed environment of smart metering.
- Use policies that are more suited to restricted devices and low bandwidths.
- Be the root of trust for its own software and firmware.
- Prior to customer acceptance, the system is owned and run by L+G
- Avoid key renewal and revocation on embedded devices

The L+G "Gridstream" components are delivered with the L+G PKI installed. However, a customer is free to replace it with a PKI of its own choice.

Depending on the market requirements, L+G may operate sub-CAs that are signed by a third parties' CA. These sub-CAs are part of a production line where key pairs that are generated inside the device and certified in a fully automated process.

The CA policies for the externally certified CAs will be determined in cooperation with the certifying CA. Where possible and practical, the L+G policy and profiles are aligned with common CA policies like the ones in [2 |]

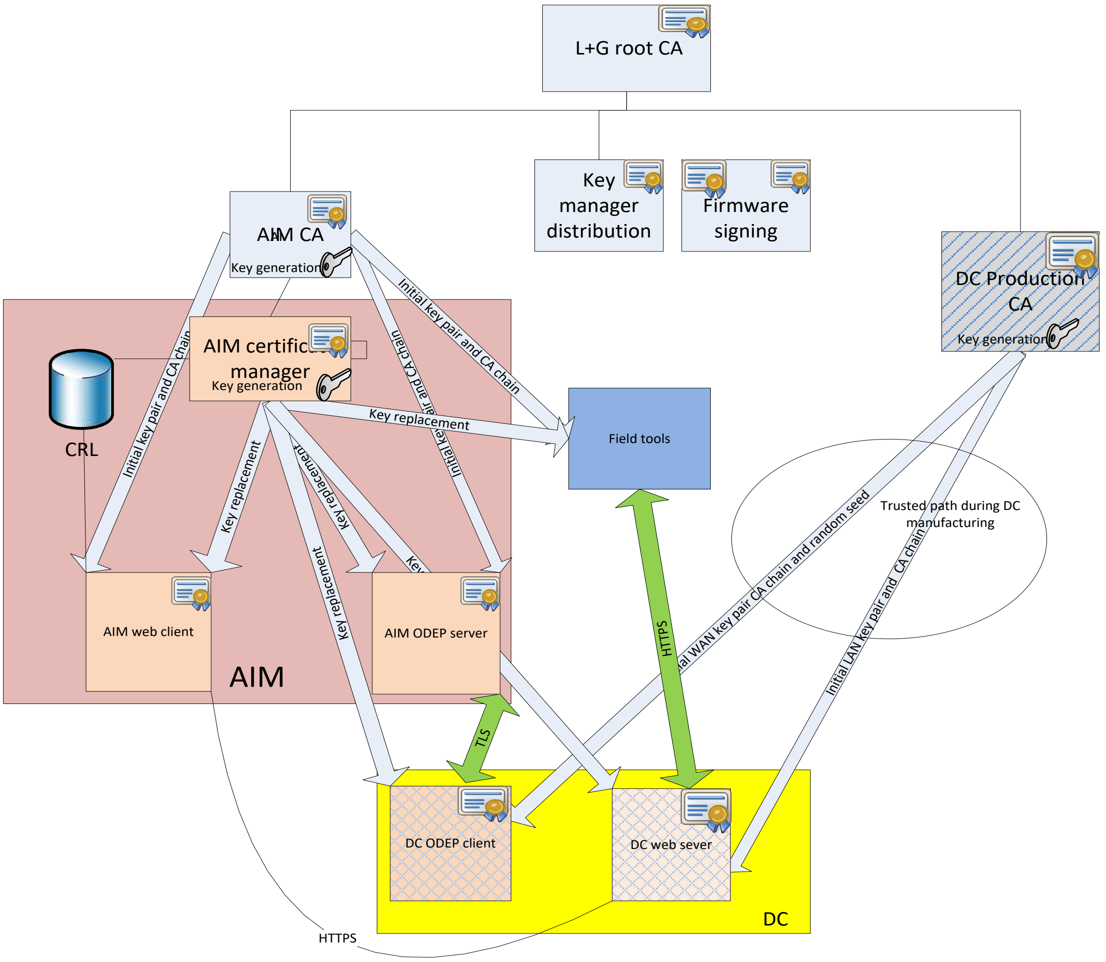

Figure 1 L+G "Gridstream" PKI Overview

2. Certificate Policy

2.1. Introduction

A certificate policy focuses on certificates and the CA's responsibilities regarding these certificates.

- A certificate policy typically answers the question about what purposes the certificate serves, and under which policies and procedures the certificate has been issued. A certificate policy addresses the following issues:
- How users are authenticated during certificate enrolment
- Legal issues, such as liability that might arise if the CA becomes compromised or is used beyond its intended purpose
- The intended purpose of the certificate
- Private key management requirements, such as storage on smart cards or other hardware devices
- Whether the private key can be exported or archived
- Requirements for users of the certificates, including how to proceed if their private keys are lost or compromised

- Requirements for certificate enrolment and renewal
- Minimum length for the public key and private key pairs
- Algorithms
- Certificate Practice Statements

2.2. Implementation

2.2.1. Site location and construction

The sub CAs are off-line whenever possible.

The private keys for the CAs are generated and stored on SafeNet HSMs.

The root CA is strictly offline. When not in use, it is stored in a secure location.

2.2.2. Certificate Validity Period

Certificates do not expire, unless required by a subordinate policy. In small, remote and unattended devices the loss of connectivity due to an expired certificate has to be prevented.

The start time of a certificate to be validated by a remote device is the earliest time the firmware initializes the real time clock of a device, unless a later date is required by a subordinate policy. This avoids starting a device with invalid certificates.

The certificates issued by the L+G PKI do not expire, thus preventing losing connectivity due to expired certificates. However, reaction to the result of failed certificate verification is the responsibility the implementer and not covered by this document. The amount of data transported during the operational lifetime of a smart metering / smart grid end device is well below the amount of data that should be encrypted with a single key (order of 2^{48} bytes).

2.2.3. Certificate use

The certificates are used to:

- Certify subordinate CAs
- Authenticate the parties in a TLS connection (TLS client and server certificates)
- Participate in the TLS session key agreement
- Signing certain user data (using CMS or DLMS “Access Service”)
- Participate in key establishment protocols
- Ensure the authenticity of cryptographic keys generated by L+G
- Ensure the authenticity of software and firmware produced by L+G

Each certificate is issued for a dedicated purpose by setting the “key usage” and the “extended key usage” attributes to the values specified in the CPS.

The private keys for the root CA are backed up to a second HSM.

The private keys of sub-CAs are neither back upped nor exported. The private keys of the sub CAs are stored in a HSM.

2.2.4. Algorithms

The algorithms offered are:

- RSA (minimum 2048 bit modulus length) with SHA-256
- ECDSA with NIST p256 and SHA-256
- ECDSA with NIST p384 and SHA-384
- SHA-1 for the 'key identifier' as in RFC 5280 and legacy browsers.

For legacy purposes, RSA is used, for newer development the algorithms from the "NSA Suite B" are used, as these are widely accepted for smart metering security.

If required, also national algorithms like "Brainpool" curves can be added.

The CAs accept CSRs in PKCS10 (RFC 2986) and CRMFs RFC 4211 formats.

2.2.5. Registration Authority

A RA is not foreseen for end user certificates. These certificates will be produced in an automated process, where the sub CA gets the data from the production line equipment via a "trusted path".

Other certificates are issued so infrequently, that the CA's crypto custodian performs the RA functions.

Keys of sub CAs are signed after an "out of band" verification of the request.

Key (transport) signing certificates are generated by the crypto custodian on reception of the purchase order if they absent or expired.

Code signing certificates are produced as part of the release process for OTA firmware updates.

CA certificates can be added OTA to a device via a secure connection.

2.2.6. Naming

The names for the issuer follows the convention that the CN of a CA ends with CA and the O ends with PKI.
The names of end devices are devices' serial numbers.

2.2.7. Roles

The roles are shaped by the capabilities of OpenSSL with a SafeNet HSM in a Windows environment.

Each sub CA shall define the following roles:

- Operator (Crypto User in SafeNet terms)
- Auditor

The Operator generates the CA key pair and the certificate signing request.
He will ask the superior CA for a certificate and import such after verification.
He keeps a list of generated CA keys and the imported certificates.

The operator will open the CA at the start of a production run and close it when not needed for production. The operator can inspect the log files to view which end user certificates are issued.

The auditor shall inspect the logs at least every 12 months; in order to verify which certificates are produced.

Such inspection shall comprise verification as to if the certificated produced match with the CPS as well as which certificates have been imported.

The role of auditor can be performed by the Operator of the superior CA. This shall ensure that the global policies are being complied with.

Every role shall have a deputy.

The roles of the (deputy) Operator and the (deputy) auditor shall not overlap.

2.2.8. Root generation ceremony

The "security officer" and "domain owner" (in SafeNet term) create the partition(s) and user tokens. It is only relevant during this step..

All 4 root CA Operators are present during the root key generation ceremony.
As part of the ceremony, each Operators is issued an access token and makes a duplicate of the access token.
The whole procedure shall be recorded on video.

2.2.9. Sub CA renewal

To prevent that the knowledge and routine about sub CA signing are lost, sub CA private keys shall be replaced on a yearly basis.

Therefore, each L+G sub CA shall generate a new sub CA key pair and send the CSR to the root CA on a yearly basis.

The root CA will sign this with the normal procedure and return the certificate to the requesting Operator. The Operators shall verify the validity of the certificate.

Only the private key is changed, the previously issued certificates stay valid.

3. Certificate Practice Statement

3.1. Introduction

The certificate practice statement (CPS) translates certificate policies into operational procedures on the CA level. The certificate policy focuses on a certificate; the CPS focuses on a CA.

A CPS for a certification authority can meet the requirements of multiple certificate policies. Each CPS contains information specific to that CA. However, the CPS for a subordinate CA can refer to the CPS of a parent CA for general or common information. A CPS may include the following types of information:

- Positive identification of the CA (including CA name, server name, and DNS address)
- The kind of certificate policies implemented by the CA and the issued certificate types
- Policies, procedures, and processes for issuing and renewing certificates
- Cryptographic algorithms, CSP, and key length used for the CA certificate
- Lifetime of the CA certificate
- Physical, network, and procedural security of the CA
- The certificate lifetime of each certificate issued by the CA
- Policies for revoking certificates.
- Policies for certificate revocation lists (CRLs), including CRL distribution points and publishing intervals

3.2. Common L+G CPS

The certificates have an unlimited validity period (unless limited by a subordinate CPS). This ensures that there is no requirement to replace certificates within the operational life of a device. The private keys of the sub-CAs are replaced yearly.

To stay secure over the long lifetime, the RSA certificates use at least a 2048 bit modulus.

The start of the validity period depends on the time management of the device, and may be set in the past.

The software signing certificates are ‘stand alone’.

The root CA uses a Pin Entry Device (PED) for access control.
The subCAs use a password based access control.

CRLs are issued when needed. There is no fixed publication interval.

Only the private keys of the root CA are backed up. If the private keys of a sub CA are lost, the responsible Operator will generate new ones and ask the Root CA for an unscheduled signature.

All Operators of the CAs are reachable over the mail distribution list: “CA.emea@ landisgyr.com”.

The DN follows the common convention where the CN of a CA end with “CA” and the O ends with “PKI”.

3.3. Root CA CPS

The Root CA resides in the one and only partition of a SafeNet Luna G5.

The Operators of the Root CA shall verify the correct functioning of the backup process once every 2 years. The backup is a cloned HSM.

Authentication is performed by a 2 out of 4 principle. All 4 Operators have a PED access token (and a copy of it).

Each Operator stores a copy of his PED off site and separate from each other.

The managers of the Operators are informed to ask the Operator to return his access tokens when the Operator leaves L+G Zug.

The root CA certifies only sub CAs and not end users.

Table 3-1 Landis + Gyr Root Certificate Profile

Attribute	***X509 Name***	***Value***
Subject	CN	Landis + Gyr Root CA
	O	Landis + Gyr PKI
	C	CH
Serial Number	SERIALNUMBER	1
Validity	notAfter	99991231235959Z
	notBefore	19700101000001Z
	KeyUsage	KeyCertSign, CrlSign
	BasicConstraints	cA=true,pathlength=2
Issuer	CN	Landis + Gyr Root CA
	O	Landis + Gyr
	C	CH
Extended Attributes	CertificatePolicies	1.3.6.1.4.1.8410.300.2.1.4.1.2 uri=www.landisgyr.com

	SubjectAltnames	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

	IssuerAltname	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

Subject:
cn = Landis Gyr Root CA
o = Landis Gyr

Algorithms:

RSA-4096 with SHA-256
RSA-6144 with SHA-256
ECC P256 with SHA-256
ECC P384 with SHA-384

Certificate Policy
OID = 1.3.6.1.4.1.8410.300.2.1.4.1.2
iso.org.dod.internet.private.enterprise.Landis & Gyr Communications SAS.PKI.CPS.x509.global.v1.2

The SafeNet “Security Officer” and “Domain Owner” use a single access token as they have no access to the data.

3.3.1. Signing the AIM sub CA signing request.

The starting date is set in the past as the certificate may have to be checked by an embedded device for which the time is not set yet.

3.3.2. Signing the DC sub CA signing request

Verify before signing that the CN="Landis + Gyr DC CA" and the OU≠TEST

The starting date is set in the past as the certificate may have to be checked by an embedded device for which the time has not been set yet.

3.3.3. Other PKIs

The root CA can issue root certificates for pilot projects and demos. These CPS will be in separate documents.

3.3.4. Site location and construction

Signing by the root CA will be performed in a meeting room in Zug.

The root CA HSM and the laptop with the CA software is stored in the fireproof safe in the secure development area in Zug when not in use.

The backup root CA HSM and a backup of the CA software (and configuration) is securely stored off site

The root CA operators keep their access tokens at a secure place and the copy locally separated. The purpose is to ensure availability if the building at Theilerstrasse 1 in Zug is destroyed.

3.4. Meter Production Sites CPS

The sub CA at the meter production site produces private keys and certificates to sign the DLMS key files to be sent to the customer.

Northfield operates according to an own policy, as described by the “Key Management Policy”, ISNS 023 (public) by Chris Notley.

3.5. DC Production Site CPS

The sub-CA at the DC production site produces random seeds, private keys and certificates for the TLS connections of the DC. The random seeds and private keys are generated by the HSM random number generator and the public key is signed by the DC sub-CA.

The DC certificates use a smaller RSA modulus, as they are easily renewable and the bandwidth and processing power of a DC is limited.

As the update of the DC software consists of normal executables, transferred over a secure connection, software signing is currently not foreseen.

The DC production sub-CA does not support OCSP. The customer’s system shall verify the CN of the WAN certificate against a white list of installed and trusted DCs, which is part of the AIM functionality.

The DC production sub-CA can issue CRLs if required. A fixed publication interval is not foreseen.

As DC connections often have a limited bandwidth, the number of attributes in the certificates is kept to a minimum.

The private key of the DC sub-CA is renewed on a yearly basis. This keeps the routine of the operator.

The DC sub-CA operator sends the CSR and the index.txt to the root CA for renewal.

Algorithms:
RSA 2048 with SHA-256
ECC P256 with SHA-256

3.5.1. DC Sub CA certificate

Table 3-2 Landis + Gyr DC CA Certificate Profile

Attribute	***X509 Name***	***Value***
Subject	CN	Landis + Gyr DC CA
	O	Landis + Gyr PKI
	C	FR
Serial Number	SERIALNUMBER	Start at 1
Validity	notAfter	99991231235959Z
	notBefore	Date of issue
	KeyUsage	KeyCertSign
	BasicConstraints	cA=true,pathlength=0
Issuer	CN	Landis + Gyr Root CA

	O	Landis + Gyr PKI
	C	CH
Extended Attributes	CertificatePolicies	1.3.6.1.4.1.8410.300.2.1.4.1.2 uri=www.landisgyr.com

	SubjectAltnames	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

	IssuerAltname	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

3.5.2. DC Certificates

The DC has 2 (physical) TLS interfaces:

1. LAN
2. WAN

Each of these interfaces has an own TLS certificate.

3.1.1.1 | Certificate Validity

notBefore: Date of issue. The DC certificates are validated by the head end system which always has the correct time.

notAfter: infinity.

3.1.1.2 | Local Ethernet (LAN) certificate

Table 3-3 Landis + Gyr DC LAN Certificate Profile

Attribute	***X509 Name***	***Value***
Subject	CN	dc450-local-port
	O	Landis + Gyr
Serial Number	SERIALNUMBER	1
Validity	notAfter	99991231235959Z
	notBefore	Date of issue
	KeyUsage	digital signature, key agreement, key encipherment
Issuer	CN	Landis + Gyr DC CA
	O	Landis + Gyr PKI
	C	FR
Extended Attributes	Extended Key Usage	Server authentication (Webserver) 1.3.6.1.5.5.7.3.1
	CertificatePolicies	1.3.6.1.4.1.8410.300.2.1.4.1.2 uri=www.landisgyr.com

	SubjectAltnames	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

	IssuerAltname	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

Algorithm RSA 2048 with SHA-256 to be able to support legacy field tools.

The “Common Name” must match the text given in the browser to enable a HTTPS connection without issuing a warning.

This interface uses a fixed IP (default 10.0.0.1), which can be changed by the customer.

The customer’s systems and tools shall maintain the relation between URI and IP address with a host file or a DNS service.

3.1.1.3 | WAN certificate

Table 3-4 Landis + Gyr DC WAN Certificate Profile

Attribute	***X509 Name***	***Value***
Common name	CN	DC’s system title
Organisation	O	Landis + Gyr PKI
Serial Number	SERIALNUMBER	1
Validity	notAfter	99991231235959Z
	notBefore	Date of issue
Issuer	CN	Landis + Gyr DC CA
	O	Landis + Gyr
	C	FR
	KeyUsage	digital signature, key agreement, key encipherment
Extended Attributes	Extended Key Usage	Server authentication (Webserver) 1.3.6.1.5.5.7.3.1 + Client authentication (Webserver) 1.3.6.1.5.5.7.3.2

Algorithms:
RSA 2048 with SHA-256
ECC P256 with SHA-256

A name resolving service (for example DNS) shall be available to AIM installations to verify HTTPS connections to the DC. AIM verifies TLS connections made by the DC by looking up the system title (CN) in a ‘white list’ of DCs belonging to the system. (Even if it is a genuine L+G DC, this does not imply it is your DC.)

3.1.1.4 | Audit

The auditor shall verify that the private key is renewed on a yearly basis, that the number of certificates shall match the number of shipped DCs and that the CNs follow the CPS. Deviations shall be traceable. Shipping more DCs than having issued certificates may indicate that more than one DC has the same key material.

.

3.6. DC Development Site CPS

To facilitate development, a second CA (collocated with the AIM sub CA) may also issue DC certificates. The policies and processes are the same, except that C=FI in the DN.

3.7. AIM CA CPS

The AIM sub CA signs the key signing certificate for the AIM certificate manager.
The private key of the AIM sub-CA is renewed on a yearly basis.

3.7.1. AIM sub-CA certificate

Table 3-5 Landis + Gyr AIM sub-CA Certificate Profile

Attribute	***X509 Name***	***Value***
Subject	CN	Landis + Gyr AIM CA
	C	FI
	O	Landis + Gyr PKI
Serial Number	SERIALNUMBER	1
Validity	notAfter	99991231235959Z
	notBefore	the earliest date set by a newly installed DC firmware. This parameter shall be determined by the DC development team as it may depend on the firmware version.
	KeyUsage	KeyCertSign, CrlSign
	Basic Constraints	cA = true path length constraint = 1
Issuer	CN	Landis + Gyr Root CA
	O	Landis + Gyr PKI
	C	CH
Extended Attributes	CertificatePolicies	1.3.6.1.4.1.8410.300.2.1.4.1.2 uri=www.landisgyr.com

	SubjectAltnames	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

	IssuerAltname	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

Algorithms:
RSA 2048 with SHA-256
ECC P256 with SHA-256
ECC P384 with SHA-384

The AIM sub-CA signs the root certificate of a third party CA for the AIM certificate manager. This is the use case when transferring the AIM root of trust from L+G to a CA chosen by the customer.

3.8. AIM certificate manager CPS

The AIM certificate manager produces the TLS keys and certificates for the HES, replacement TLS certificates for the DC and web client certificates for field tools.

3.8.1. AIM certificate manager certificate

Table 3-6 Landis + Gyr AIM Certificate Manager Certificate Profile

Attribute	***X509 Name***	***Value***
Subject	CN	AIM Certificate Manager
	C	*Customer specific*
	O	*Customer specific*
Serial Number	SERIALNUMBER	1
Validity	notAfter	99991231235959Z
	notBefore	the earliest date set by a newly installed DC firmware. This parameter shall be determined by the DC development team as it may depend on the firmware version.
	KeyUsage	KeyCertSign, CrlSign
	Basic Constraints	cA = true path length constraint = 0
Issuer	CN	Landis + Gyr AIM CA
	O	Landis + Gyr PKI
	C	FI
Extended Attributes	CertificatePolicies	1.3.6.1.4.1.8410.300.2.1.4.1.2 uri=www.landisgyr.com
	SubjectAltnames	*Customer specific*

	IssuerAltname	uri=www.landisgyr.com
		email=CA.emea@ landisgyr.com

3.8.2. Certificates issued by the AIM certificate manager

The customer may set the validity period to any value of his choice. One option is to issue web client certificates with a short lifetime to provide a lazy revocation mechanism for field tools. If the customer does not specify a certificate lifetime, the start date will be the UTC of issue and the validity will be infinite.

3.1.1.5 | Certificate attributes

Key Usage (Restriction) = digital signature

Extended Key Usage = Server authentication (Webserver) 1.3.6.1.5.5.7.3.1 and/or
Client authentication (Webserver) 1.3.6.1.5.5.7.3.2

3.8.3. Certificates Revocation Lists issued by the AIM certificate manager

The customer may use the AIM certificate manager to issue CRLs for his own IT environment.

3.9. Software Signing CPS

Extended Key Usage (2.5.29.37) = Code signing (1.3.6.1.5.5.7.3.3)

For software signing, 2 key pairs shall be used;

1. Developer pair
2. Release pair

The developer pair is made available to all developers. In this way, signed software updates can be integrated and tested in an early stage.

The release private key is only used to sign official releases, according to the processes described in **Error! Reference source not found.**.

4 | Introduction to PKI

There has always been a need to send messages between parties where these messages have to be protected against unauthorized changes or unauthorized reading.

Cryptography is a technique to prevent messages being read by unauthorized parties.

Cryptography uses an ‘algorithm’ (a series of mathematical operations) to change a message from a plain text to a cipher text (encryption) and back again (decryption).

The algorithm is parameterized by a ‘key’ which is shared among the communicating partners. Only with the correct key, the algorithm can transform a cipher text back to the original plain text

The problem remains how to exchange the key securely with the communication partners, as anyone who gets a copy of the keys can decipher all subsequent messages.

4.1 | Public Key cryptography

Cryptographic algorithms can be divided in 2 categories:

1. Symmetric, where the same key is used for encryption and decryption.
2. Asymmetric, where different keys are used for encryption and decryption. These 2 keys are mathematically related.

The 2 keys for an asymmetric algorithm are called the “public key” and the “private key”. The design of the algorithm ensures that it is not possible to derive the private key from the public key.

This can solve the problem of getting the key securely to the communication partner.

The opposite operation from encryption is signing; Alice uses her private key to sign a message and the whole world can use Alice’s public key to verify the signature.

To give an example:

Alice[1] wants to send a secret message to Bob.
Alice asks Bob for his public key.
Bob sends his public key to Alice
Alice uses Bob's public key to encrypt her message
Bob uses his private key to decrypt Alice's message.

This is the idealized case. In the next case, Mallory wants to read the message as well.

Alice wants to send a secret message to Bob.
Alice asks Bob for his public key.
Mallory intercepts Alice's request for the key.
Mallory asks Bob for his public key
Mallory sends his public key to Alice pretending it is Bob's key.
Alice uses Mallory's public key to encrypt her message (believing it is Bob's public key)
Mallory intercepts Alice's encrypted message.
Mallory uses his private key to decrypt Alice's message.
Mallory uses Bob's public key to encrypt Alice's message
Bob uses his private key to decrypt Alice's message.

As a public key is just a (large)number, it is not possible to see who 'owns' the matching private key. The scenario above is called a 'Man in the middle' attack.

4.2 | Certification Authority

To avoid this attack, Alice and Bod agree on a trusted third party, Trent. Bob gets Trent's public key in a reliable way.

Alice presents her public key and a proof of identity to Trent.
Trent uses his private key to sign Alice's public key together with her identification.

This signed pair of key and identity is called a 'certificate' and the usual name for this type of trusted third party is a "Certification Authority". The verification of the identity can be done separately by a "Registration Authority".

The rules that Trent uses to confirm Alice's identity are part of the "Certificate Policy" and these determine how much trust can be placed in the certificate. For example, asking for a certificate only by e-mail is less trustworthy than presenting yourself with your passport at the RA.

4.3 | How does a public key algorithm work.

The Diffie Hellman algorithm (from 1976).

Alice and Bob select two large (500 to 1000 digits) numbers G and m from a kind of catalogue. These are called the "Domain parameters".

[1] The actors in cryptographic use cases are commonly called Alice,Bob, Mallory, Trent.

Alice generates a large random number $a < m$, which will be her private key.
Bob generates a large random number $b < m$, which will be his private key.

Alice raises G to the power a modulo[2] m. This number $A = (G^a \; mod \; m)$ will be her public key.

Bob raises G to the power b modulo m. This *number* $B = (G^b \; mod \; m)$ will be his public key.

Alice and Bob exchange their public keys A and B.

Alice raises B to the power a modulo m. The number $K = (G^{ab} \; mod \; m)$ will be the shared key.

Bob raises A to the power b modulo m. The number $K = (G^{ab} \; mod \; m)$ will be the shared key.

The mathematical trick is, that even if an attacker knows m, G and G^a, he cannot calculate a, as ${}^G log(A) \; mod \; m$ (the inverse operation of A = $G^a \; mod \; m$) is very difficult for the right choice of G and m.

4.4 | What does a certificate look like

In human readable form:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
  Signature Algorithm: ecdsa-with-SHA256
    Issuer: C=CH, O=Landis + Gyr PKI, CN=Landis + Gyr Root CA
    Validity
      Not Before: Jan  1 00:00:00 1970 GMT
      Not After : Dec 31 23:59:59 9999 GMT
    Subject: C=CH, O=Landis + Gyr PKI, CN=Landis + Gyr Root CA
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
        Public-Key: (256 bit)
        pub:
          04:46:c8:2c:6e:b6:1d:07:ce:1f:f9:7f:3e:46:73:
          69:53:3c:0e:63:0b:43:ba:46:d8:ac:11:99:98:a2:
          85:55:84:be:d0:19:37:ae:36:3a:46:9c:8c:5c:1f:
          3b:bc:f4:4d:68:3e:08:7c:c7:8e:a1:2b:d4:52:e2:
          d8:20:c8:73:13
        ASN1 OID: prime256v1
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:2
      X509v3 Subject Key Identifier:          BA:10:31:B3:E0:82:D0:7C:A0:24:8E:EB:69:6A:B7:02:93:D4:89:A1
      X509v3 Authority Key Identifier:
keyid:
BA:10:31:B3:E0:82:D0:7C:A0:24:8E:EB:69:6A:B7:02:93:D4:89:A1
```

[2] Subtract m as many times from the result till it is between 0 and m. It is like operation on a clock, 13 hours after 1 o'clock it is 2 o'clock. A clock operates „modulo 12".

```
         X509v3 Key Usage: critical
             Certificate Sign, CRL Sign
         X509v3 CRL Distribution Points:
             Full Name:
               URI:http:/www.landisgyr.com/ca/emea/ca.crl
         X509v3 Subject Alternative Name:
             URI:http://www.landisgyr.com/
         X509v3 Issuer Alternative Name:
           URI:http://www.landisgyr.com/,mail:ca.emea@landisgyr.com
         X509v3 Certificate Policies:
             Policy: 1.3.6.1.4.1.8410.300.2.1.4.1.2

    Signature Algorithm: ecdsa-with-SHA256
        30:44:02:20:6e:f3:b1:9f:f8:c9:ce:11:d3:06:78:d6:dc:9c:
        92:08:f9:f2:42:9d:69:92:1d:55:bd:4c:d3:7b:64:da:8d:23:
        02:20:18:47:6e:0d:c3:01:41:62:e1:bc:50:e9:d1:2f:d3:08:
        cf:c7:48:ee:8f:b1:8b:b8:8b:5b:ed:55:0c:e9:e6:d1
```

The same certificate in machine readable form:

-----BEGIN CERTIFICATE-----
MIICozCCAkqgAwIBAgIBAjAKBggqhkjOPQQDAjBHMQswCQYDVQQGEwJDSDEZMBcG
A1UECgwQTGFuZGlzICsgR3lyIFBLSTEdMBsGA1UEAwwUTGFuZGlzICsgR3lyIFJv
b3QgQ0EwIhgPMTk3MDAxMDEwMDAwMDBaGA85OTk5MTIzMTIzNTk1OVowRzELMAkG
A1UEBhMCQ0gxGTAXBgNVBAoMEExhbmRpcyArIEd5ciBQS0kxHTAbBgNVBAMMFExh
bmRpcyArIEd5ciBSb290IENBMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAERsgs
brYdB84f+X8+RnNpUzwOYwtDukbYrBGZmKKFVYS+0Bk3rjY6RpyMXB87vPRNaD4I
fMeOoSvUUuLYIMhzE6OCASEwggEdMBIGA1UdEwEB/wQIMAYBAf8CAQIwHQYDVR0O
BBYEFLoQMbPggtB8oCSO62lqtwKT1ImhMB8GA1UdIwQYMBaAFLoQMbPggtB8oCSO
62lqtwKT1ImhMA4GA1UdDwEB/wQEAwIBBjA3BgNVHR8EMDAuMCygKqAohiZodHRw
Oi93d3cubGFuZGlzZ3lyLmNvbS9jYS9lbWVhL2NhLmNybDAkBgNVHREEHTAbhhlo
dHRwOi8vd3d3LmxhbmRpc2d5ci5jb20vMDsGA1UdEgQ0MDKGGWh0dHA6Ly93d3cu
bGFuZGlzZ3lyLmNvbS+BFWNhLmVtZWFAbGFuZGlzZ3lyLmNvbTAbBgNVHSAEFDAS
MBAGDisGAQQBwVqCLAIBBAECMAoGCCqGSM49BAMCA0cAMEQCIG7zsZ/4yc4R0wZ4
1tyckgj58kKdaZIdVb1M03tk2o0jAiAYR24NwwFBYuG8UOnRL9MIz8dI7o+xi7iL
W+1VDOnm0Q==
-----END CERTIFICATE-----