Certificate Services

The foundation for building trust in a connected world

THE FOUNDATION FOR BUILDING TRUST

Trust is the key word for most organizations and processes. We need to be able to trust that the person who accesses our systems and signs an agreement is who she claims to be. That a machine or device in an Internet-of-Things solution is what it says it is. That the data one system sends to another is the right data, with its integrity intact.

A vital part of building a complete cyber security solution is making sure that resources and people can be trusted. Trusting the wrong person, data or machine could have very serious repercussions. The way to solve this security issue is by building and ensuring trust using certificates.

A certificate is a small computer file with encrypted information providing a way to ensure the identity of people, resources and data. It is managed by the certificate infrastructure and can be generated internally for intra company resources, or externally by a trusted partner for external use like web servers.

TRUST AND COMPLIANCE

To be able to comply with new and evolving regulations, the need for encryption, strong authentication, and signing of data has increased. More and more, organizations are discovering that it is both challenging and time-consuming to maintain an internal Trusted Certificate Authority infrastructure, and with changing threats and business needs, staying safe and compliant is a moving target.

CGI Certificate Services is a hosted solution where CGI handles the entire infrastructure and all the maintenance work needed for a secure and sustainable solution. It also maintains the operations- and issuing policies so we know what trust a certificate has.

The solution is based on a platform with a number of add-ons and is easy-to-use, simple to manage and highly flexible for adaptation to any customer's unique environment.

CERTIFICATE SERVICES

- Easy and secure access
- Clients' certificate authorities' key secured by HSM modules
- Secure and reliable from day one
- Short deployment time by using existing certificate platform
- Flexible delivery model, multi-sourcing.
- Reduce total cost of ownership with an end-to-end solution from a single vendor
- Service operation according to ETSI TS 102 042 specification, continually adapted to new standards ETSI EN 319 401 and the issuing process can be adapted to map LOA Level 3 or 4 according to NIST 800-63 or Substantial or High according to eIDAS.

Physical Security
Everything starts here. With physical security from the datacenter to the operation room of the service.

Logical Security
The logical security need to be built hand in hand with the physical, in layer after layer to protect the keys.

Operational Security
Professionals that operate the certificate service are classified as trusted, with passed training and back-ground verification.

Processes and validation
The process and policy of end-user validation and issuing need to define the trust of a Digital certificate ecosystem.

Subscriber Security
Ensuring that end-user keys are secured and implementation of a key management policy on the servers and/or devices

European standard for Electronic Signatures and Infrastructures
ETSI EN 319 401 – General Policy Requirement for **Trust Service** Providers

END-TO-END CERTIFICATE SOLUTION

Certificates are issued in a variety of different formats and for many different end-use cases. CGI offers a range of different alternatives that can map international standards for identity issuing, such as NIST 800-63, eIDAS or similar standards, and are capable of issuing certificates for computers, users, servers and devices.

The user and device certificates are issued for internal use and every company is in charge of their own section of the service. For server certificates, customers can get both publicly trusted certificates from an external provider, or internal - not publicly trusted - from their own section of the service.

CGI Certificate Services is a turnkey solution where all parts, such as certificates, smart cards, middleware, certificate client software, and administration tools, is delivered and supported from a single provider. The fact that CGI handles the complete solution, reduces both the deployment time and the cost of maintenance and support.

The services also include administration tools and reports needed to be compliant according to international standards for certificates and digital identity issuing.

The server solution is highly flexible and customer can grow and expand their Certificate Authority tree easily via a change request to the service. Also, adding new certificate profiles or templates is easy to order via change.

> *Sustainable security demands changes almost every day. Agile way of working effects the foundations for security such as digital certificates and increases the need of flexibility in the trust services. Without a flexible service, there is a higher risk that organizations implement complex workarounds that in the end creates a security vulnerability.*

Automated certificate delivery

Certificate Services offers auto-enrollment of certificates for users, computers and devices. This is an add-on feature, providing automatic installation and updating of certificates. This is often preferred on secure networks, which require a valid certificate for users and/or computers.

Which users and computers that are in need of certificates, and what level of access they should be allowed, is controlled using groups in the customer's Active Directory.

CGI supports Windows, OS/X and Linux clients with auto-enrollment of device certificates.

For Windows user there is an auto-enrollment of S/MIME e-mail signing and encryption certificates. They can be enrolled via the internal trusted certificate authority or – if needed - external public trusted certificates.

ICGI's client also configures the end-user Outlook client so users do not need to manually change their Outlook client when using S/MIME. A key recovery function helps users when they reinstall or change their computer.

To be able to verify certificates, network equipment needs a RADIUS service. If such a service is not already available at the client, CGI can provide that as well.

The ITSM integration means that a server certificate request can be approved in the ITSM tool and thereby follow the company's ITIL process. When a certificate is about to expire, the system automatically asks for re-approval and the server can, via a REST API, get the renewed certificate after it has been approved in the ITSM tool.

Smart card support

Smart cards can be used to enhance the security in a company by providing strong authentication for employees or B2B partners. Certificate Services offers a complete lifecycle management for certificates stored on smart cards as an add-on feature, which makes it easy for companies to start using them in their organization.

Mobile device support

The growing mobility demand from the business is sometime a cybersecurity challenge. To combine a mobile device management solution with CGI Certificate Services and distribute certificates to the devices will increase the security in many ways.

It is also possible, as an example, to start using certificate-based authentication for e-mails and calendar mobile synchronization services. In addition, you can get better control over which mobile device are allowed to connect to the company's wireless network.

SERVER CERTIFICATES WITH THE CORRECT TRUST

An organization today normally needs internal trusted server certificates for servers that are only exposed internally or use an internal DNS name. Servers that are used for services exposed publicly need digital certificate from publicly trusted Certificate Authority. CGI Certificate Service has integrated our solution so you can use CGI Certificate Service administrative interface to enroll for public trusted server certificates.

This gives an organization one end-to-end solution for the management of server certificates. Each customer need to have an agreement with a public certificate issuer, and CGI Certificate Services integrates our solution the public certificate authority via an API. If only internal trusted server certificates are issued, the customer can use the same administrative interface. We offer one solution and one interface for management for both internal server certificates as external publicly trusted.

FLEXIBLE DELIVERY MODELS

CGI offer the service as SaaS delivery, client dedicated hardware and software service delivery from CGI or On-perm delivery when operation of the service is made remotely via CGI high security certificate operation center in Sweden.

HOW TO GET STARTED?

1. Meeting with experts

Discuss digital certificate topics and **how you could improve your organization's trust** in a meeting with CGI experts.

2. Design

Workshop with - and/or visit - our certificate service team in Stockholm with your management team and system security architect. In this workshop we discuss the design and type of service delivery your organization need.

3. Proposal

Based on the workshop you receive **proposal** that cover the design of a flexible and trusted certificate service.

CGI

CONTACT

Gunnar Klintberg
Digital Certificate and Signatures expert
gunnar.klintberg@cgi.com
+46 8 671 0371

Christer Samuelsson
Cybersecurity expert
christer.samuelsson@cgi.com
+46 8 51767327

www.cgi.se/cyber
www.cgi.com/cyber