

Contact: John Tunstall
Global Trust Authority
Phone: +32 2 211 1102
Address: Marie Thérèse 11
1000 Brussels, Belgium

john.tunstall@gta.multicert.org

PRESS PACK

Information about the Global Trust Authority (GTA)

Version 1.0 / 27-Sept-01

Contents

1. <i>GTA Introduction</i>	2
2. <i>GTA organisation and history</i>	3
3. <i>Membership</i>	5
4. <i>Current list of GTA members</i>	7
5. <i>Working of GTA</i>	8
6. <i>Basics of the liability model</i>	11
7. <i>Programs</i>	12
8. <i>Applications</i>	13
9. <i>GTA's Market approach</i>	15
10. <i>GTA and the European Commission</i>	16
11. <i>Market developments</i>	18
12. <i>About digital signatures</i>	20
13. <i>GTA Glossary</i>	22

1. GTA Introduction

Background

The Internet offers the opportunity for a wide range of global e-services (e-commerce, e-payment, e-business, etc.) for many organisations, in the Consumer as well as Business sectors. E-services can be accessed through many environments, like mobile phones, Personal Digital Assistants, Interactive Television and Personal Computers. These e-services need underlying functions that guarantee the credentials of the parties in a transaction, the electronic equivalent of existing contractual relationships. Users of e-services need mechanisms that provide reliable on-line identification and authentication of the participating parties in the transaction and a means of redress if the mechanisms fail. Technology known as Public Key Infrastructure (PKI)¹ can facilitate these requirements through the creation of certificates for unambiguously identifying end-users.

The majority of current PKIs accepting liability are for closed user groups, for parties wishing to subscribe to a particular scheme or on the basis of national boundaries. Interoperability, on a global and cross-sector/cross-scheme basis, is not widely catered for. There is, therefore, a need for an entity that can enable, in the virtual world, the interoperability that is already evident in the real world. The Global Trust Authority (GTA) is such an entity. GTA provides a structure for interoperable e-services that will not be distorted by the requirements of a single scheme.

GTA Proposition

The Global Trust Authority (GTA) is a not for profit, co-operative grouping, currently comprising financial sector institutions or associations. The GTA is registered in Belgium as a Limited Liability Co-operative Company and the office is located in Brussels. Among the founding members of GTA are financial institutions from Belgium, France, Italy, Portugal, Spain, and The Netherlands. The founding members represent in excess of 800 banks. Membership can be extended to other sectors subject to Board decision on a case by case basis.

Mission statement

The GTA provides an infrastructure of trust that can be used by all sectors, to conduct **cross border e-business** in a secure environment, where the liability incurred at both ends of the transaction chain is respected.

¹ See section 12, About digital signatures, for an explanation of PKI.

2. GTA organisation and history

A Managing Director, assisted by an Office Manager, leads the day to day operations of the GTA. A Technical Manager is responsible for the development and control of the necessary technical infrastructure. Strategic decisions are made by a Board, with representatives of the members. One of the members provides the Chairman. A Board Strategic Committee addresses aspects of policy and strategy in between Board meetings which take place four times a year. Working groups, consisting of volunteers from the members, carry out development work on policies, technology, legal issues and marketing. For special tasks, freelance consultants are hired on a temporary basis.

- Managing Director: John Tunstall
- Technical Manager: Liaquat Khan
- Office Manager: Veerle Gyselings
- Chairman of the Board: Jose Gabeiras
- Vice Chairman of the Board: Yves Gailly

Headlines of GTA's history

January '98	First informal meeting between a group of bankers to the creation of a body for secure cross border e-services
June '99	Start of working groups on Legal, Technical, Policy and Marketing issues
Sept. '99	The setting up of the GTA is announced in the press
January '00	ISIS Proposal issued to the European Commission
April '00	Start of Test-bed
July '00	Funding awarded by the European Commission for ISIS project
August '00	The GTA is officially registered as an Scrl in Belgium; press release issued
Sept '00	Interpay selected to operate the GTA root key facility
Sept '00	Promotion of GTA at SIBOS
January '01	Launch of Recognised Provider Program
March '01	GTA Rule Book completed
June '01	Launch of Accredited Application Program
April '01	IST Proposal issued to the European Commission together with FINREAD

August '01	Test bed completed
Sept '01	GTA Going into production key mode
October '01	GTA Live! Trusted Link and Secure it! programs announced at SIBOS

3. Membership

GTA membership is currently a regulated financial institutions involved in deposit taking, trust, securities or insurance operations or a group in which regulated financial institutions are engaged. These are typically Banks, and Banking Associations, Certificate Authorities in which the financial sector is involved. Insurance Companies, Pension Funds and Stock Exchanges may also be members..In addition membership can be extended to other sectors subject to Board decision on a case by case basis.

All new bank members are to pay a contribution rate of €20.000 for the period 2001/2002.

Benefits for members

Benefits for parties that become GTA member are:

- Full access to GTA technology, policies, legal knowledge, etc.;
- Allowed to use the GTA infrastructure, including:
 - ◆ Ability to start an MTA and offer certification services to STAs;
 - ◆ Start one or more STAs to issue GTA-branded certificates to end-users
- Ability to have applications accredited for use amongst those participating in the GTA, including the use of a library of harmonised attributes;
- Ability to co-operate in cross-border schemes together with other GTA members;
- Access to a large potential market for applications;
- Possibility to cross validate current PKI certificates into the GTA infrastructure, without issuing new certificates directly linked to the GTA-root;
- Profit from co-operation with GTA's partners, possibly from other sectors;
- Access to Recognised Providers to assist implementation and be sure that they deliver GTA-compatible products or services;
- Publicity through GTA's Marketing and PR campaigns.

Founding members in addition have:

- An automatic seat on the board, including full voting rights and influence on future membership;
- Use of the term 'GTA founding member' in publicity.

Parties who have an existing Public Key Infrastructure (PKI) in place can make use of GTA's cross validation system. This means that, without immediately becoming a member and issuing new certificates, relying parties from both the external PKI and the GTA structure can transparently validate certificates issued to end users under both PKI's.

4. Current list of GTA members

The founding members of GTA are:

- Associazione Bancaria Italiana, Italy;
- Banesto, Spain;
- BBVA, Spain;
- BNP Paribas, France;
- BSCH, Spain;
- Cartes Bancaires, France;
- Iberion, Spain;
- Interpay, The Netherlands;
- Isabel, Belgium;
- La Caixa, Spain;
- Sermepa, Spain;
- Società Interbancaria per l'Automazione SpA, Italy;
- Sociedade Interbancária de Serviços, Portugal;
- Société Générale, France.

5. Working of GTA

The GTA enables participating trading parties to establish a trusted electronic relationship. An environment is provided in which transacting parties have confidence that each party is authenticated and where limited liability can be guaranteed.

The basis of the GTA is a Scheme Trust Authority (STA) offering an application (as part of a scheme) to end-users. To be able to use this application securely, the end-user receives a digital certificate. STAs are certified by a Master Trust Authority (MTA) in their own country or region. MTAs are certified by the GTA, which is the top of the trusted hierarchy called the root. Because all parties under the GTA-umbrella trust this root, trusted relationships between all parties in the chain are guaranteed.

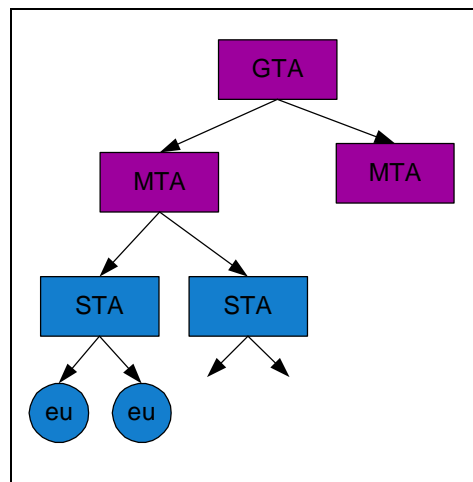


Figure: The GTA hierarchy

Validation model

An authorised relying party (ARP)² receives, for example, a signed e-mail message from an end-user (end-user 2 in the example below). The chain of certificates up to the root is attached to the message. To check if all certificates in the chain are still valid (not revoked), the ARP sends an OCSP³-message to its Validation Authority (VA); VA2 in this case. For certificates where VA2 is not authoritative, the VA sends a request to VA1, who's location is indicated in the certificate. VA1 will then return a message

² An ARP is an end-user that has a contractual relationship with an STA.

³ Online Certificate Status Protocol (OCSP) is a protocol for determining the current status of a digital certificate, which is more timely than use of CRLs.

with the current status of the certificate in question. For a certificate for which VA2 is authoritative, it will check the serial number against an up-to-date copy of the revocation list. Having determined the response of all the certificates originally requested by the relying party, VA2 sends a response message back to the ARP. If any of the certificates is identified as revoked or unknown, then the relying party should reject the transaction initiated by the end-entity.

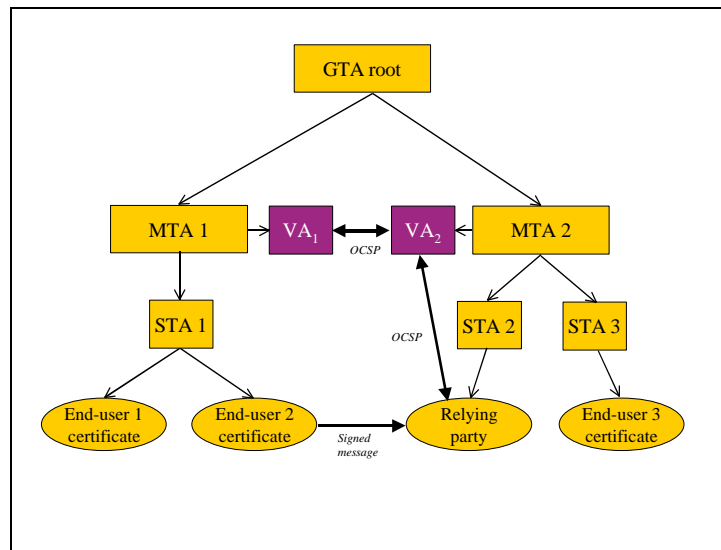


Figure: Validation example

GTA’s cross-validation concept also makes it possible for ARPs from an external PKI to validate certificates issued by a body within the GTA hierarchy and, the other way around, for GTA ARPs to validate certificates issued under the auspices of the external PKI.

Relying parties outside of the GTA infrastructure (without a contractual relationship with a GTA member or partner) are able to validate certificates for identity only. The relying party can check authenticity of the certificate chain up to the GTA root by viewing the relevant ARL/CRLs. It is the responsibility of the relying party to check the latest revocation information.

GTA’s service offering

Services of the GTA are, to:

- Create and manage the global root key, which is the basis for the secure infrastructure;
- Create a minimum set of rules for those operating under the GTA umbrella, to guarantee interoperability and integrity;

- Issue ID certificates to MTAs, provide guarantee of their identity and therefore accept limited liability;
- Maintain a list of revoked MTA-certificates;
- Act as an arbitrator of last resort for disputes between parties in the GTA-hierarchy.

6. Basics of the liability model

The following section provides a general overview of the liability model that will apply to all participants under the GTA infrastructure (i.e. GTA and each MTA and STA). This section does not constitute legal advice and the exact nature and scope of the liability of each participant under the GTA infrastructure will be set out more fully in each such participant's CPS, CP, agreements with its End Entities and/or agreements with Relying Parties.

The basic elements of the general liability model are as follows:

- Trust Authorities (TAs) are generally required (subject to a few exceptions and subject to certain value limitations) to assume liability for loss or damage suffered or incurred by any Relying Party who relied on an Identity Certificate issued by that TA, to the extent that such loss or damage arise from negligence on the part of the TA in question. Specifically, all TAs will be required to accept liability for loss or damage suffered by such Relying Parties where the loss or damage in question was caused as a result of any of the following:
 - Where the information contained within an Identity Certificate issued by the relevant TA was incorrect at the time of issuance thereof and where the relevant TA negligently failed to notice that the information was incorrect;
 - Where the relevant TA failed to use reasonable endeavours to verify the authenticity of any documents presented to it by a prospective End Entity on which that TA relied on to establish that End Entity's identity;
 - Where the TA failed to comply with its registration process (as published in its CPS and/or CP); and
 - Where the TA failed to comply in a timely fashion with any request or requirement for the revocation of an Identity Certificate issued by it.
- A TA is entitled, to the extent permitted by any applicable law, to exclude its liability for loss of profits or for indirect or "consequential" loss or damage, and also to exclude liability for loss or damage caused by events of *force majeure*.
- A TA may limit its liability in accordance with the purpose for which any Identity Certificate is issued to subordinate TAs or End Entities.

7. Programs

GTA offers three programs that are intended to assist members in the use of the GTA infrastructure.

Recognised Provider Program

Vendors who are able to offer products or services that facilitate the implementation of the GTA architecture are invited to participate in the GTA Recognised Provider Program. These products and services are diverse and cover aspects such as technical products, legal advice and general consulting. Members of the Recognised Provider Program have to meet criteria set by the GTA. A list of Recognised Providers is available on the GTA website.

Accreditation of Applications Program

Each new application wishing to operate under the GTA umbrella will be tested, to ensure that the application meets the GTA rules and technical requirements. An accredited application operates successfully across the spectrum of the membership. The GTA keeps a register of accredited applications that is available via the GTA website to those operating in the hierarchy. GTA will also maintain an attribute library with attributes used in the applications.

Secure it! Developer Program

The purpose of the *Secure it!* program is to make available a broad portfolio of applications that use the GTA trust infrastructure. *Secure it!* is designed around a 'Developer Program' to make it as easy and attractive as possible for those who wish to operate under the GTA to commence activity. Therefore *Secure it!* provides the tools, technologies and support for applications to become GTA enabled. Elements of the "*Secure it!*" program are:

- Toolkit for new member integration;
- Software developers program;
- "*Secure it!*" seminar;
- Support desk.

8. Applications

Applications based on GTA-certificates can exist within all sectors (Business to Business, Business to Consumer, Administration to Consumer, Administration to Business and Administration to Administration). Business areas where applications based on the GTA infrastructure are likely to be beneficial are:

- e-mail;
- home banking;
- Letter of Credit;
- EDI messages;
- tax declarations;
- procurement;
- e-shop;
- cross border payments;
- auctions;
- tenders;
- orders;
- invoices;
- contracts;
- proxy voting;
- secure downloading of applets to devices;
- link to Automated Clearing House;
- GSM (WAP).

Example applications

Below are a few examples of possible uses of the GTA infrastructure:

- Signing of an electronic document

A PKI smart card application with a GTA certificate can be used to digitally sign and send an electronic document, for example a proxy voting form. The sender signs the e-mail containing the proxy voting form by entering the correct 'passcode' which is verified by the GTA PKI application on the smart card. The electronic signature is generated by the application on the smart card and attached with the certificate to the e-mail. The receiving party can automatically verify that the

sender's private key generated the signature. This provides confidence that the e-mail contents are unchanged and that the sender's identity was issued by an organisation trusted by the recipient.

- Secure downloading to a device

The GTA infrastructure can be used to securely download applications to a device, in particular a chip card reader. Banks can then share one chip card terminal so that customers of one bank can use their terminal for applications from another bank. For example, a customer of Bank A wishes to send a secure instruction to initiate a financial transaction to his bank, using a chip card reader owned by Bank B. The customer inserts the smart card in the reader and there's a 'handshake' to verify that the reader and the smart card are recognised. The request for the appropriate applet is initiated and the reader sends the request along with the reader id. The repository where the signed applets of all banks are stored locates the relevant applet, encrypts the applet with the unique key of the reader and sends it to the reader. In the reader the applet is decrypted and the signatures are checked. Now the set up is complete and the transactions can happen.

- Multi application chip card

This example is based on a Master Card MULTOS v4 chip card with two applications, the MCI M/Chip application to enable secure EMV consumer shopping and a GTA compliant PKI application, to support secure e-business applications. The GTA PKI application enables the cardholder to perform various e-business functions, such as securing access to private websites, 3 domain secure SSL, digital signing of documents and e-mail, and electronic message encryption. A possible business application can be in the insurance market where a customer is able to electronically sign an insurance form and authorise the payment for the cover immediately.

9. GTA's Market approach

The basic elements of GTA's marketing efforts are:

1. Acquire new members.
2. Deploy relations with vendors in order to seek their support in the provision of products that meet the needs of GTA-members. This is done through the Recognised Provider Program.
3. General marketing/PR to create awareness in the market by issuing leaflets, maintaining a website, placing advertisements, presentations at seminars and stands at exhibitions.
4. Lobbying with at least the following organisations:
 - European Commission;
 - Comité Européen de Normalisation;
 - Central Banks;
 - National Governments;
 - ISO.

10. GTA and the European Commission

GTA actively co-operates with the European Commission, which has resulted in several initiatives.

Directive on Electronic Signatures

In 1999 the European Commission accepted the Directive on a “Community framework for electronic signatures”. All member states have to implement this Directive in their own legislation. Basically, member states ensure that electronic signatures have the same legal status as hand-written signatures, if they are based on a qualified certificate and created by a secure-signature-creation device. Furthermore, an electronic signature is not denied legal effectiveness solely on the grounds that it's in electronic form, not based on a qualified certificate or not created by a secure device. GTA will comply with and promote the European Directive on Electronic Signatures.

ISIS

In 2000 GTA was awarded funding from the European Commission within the ISIS (Standardisation Projects for the Information Society) Program, for the project **Interoperable use of certificates by means of the Global Trust Authority (GTA)**. The objective of this project is to ensure world wide interoperability between different business applications (schemes) from different Certification Authorities. This interoperability is created by implementing existing industry standards, guidelines, directives and market solutions within a hierarchical structure, called the Global Trust Authority. The project results in a trial, to test the implemented standards and policies in a real life situation. The results are used to form the definitive GTA Infrastructure, that is able to facilitate interoperability of certificates from all CAs world wide.

IST/Trusted FINREAD

GTA together with members from the FINREAD consortium, manufacturers and international payment systems, have issued the “Trusted FINREAD” proposal to the European Commission. Funding is asked from IST (Information Society Technologies) under the Fifth framework programme. The main objective of Trusted FINREAD is to define the certification procedures for FINREAD chip card readers. This creates a trusted environment where certified and signed applets can be downloaded to the FINREAD chip card readers. For the certification, Trusted FINREAD relies on the GTA to provide the necessary CA infrastructure. The second objective is to deploy a pilot where FINREAD compliant

prototypes operate within the certification infrastructure, to validate the complete FINREAD solution. The pilot will show how software applets from different CAs are interoperable in chip card readers issued by different manufacturers. A pilot with 150 prototypes is planned to operate within a fully-fledged certification infrastructure.

11. Market developments

The developments, relevant to the market segments upon which the GTA is currently focussing, are:

EMV initiative

The European banks are in the process of deploying the specification (called EMV) for chip cards, as agreed by the Card Associations. This means that businesses and consumers will receive a new card over the next 36 months, which can carry a digital certificate. In addition all European POS devices at merchants along with ATM devices will be upgraded to read the new cards. It will be up to the card issuers to decide which target customer group to issue cards to first.

Wireless data rollout

All the European mobile operators have announced wireless data services based on GPRS, generally known as 2.5G. Whilst there has been considerable attention to the 3G licences and the costs of bringing 3G to market, this has overshadowed the market introduction of 2.5G, which provides wireless internet connection for mobile devices. When used in conjunction with Bluetooth (a personal area network or PAN) it means that a range of PDAs can be used with the new generation of phones to send and receive data. Since mobile phones already carry identity, they can be used as authorisation devices for consumer and business transactions.

S.W.I.F.T.

S.W.I.F.T. is a not for profit association owned by banks. It operates the S.W.I.F.T. private network which provides secure messaging between the majority of banks and other financial institutions. S.W.I.F.T. also takes responsibility for the definition of message types. They have announced a move to IP called SwiftNet which will be outsourced and managed by Global Crossing. Those operating under the GTA root will use SwiftNet whenever this is appropriate.

Identrus

Identrus is a for profit company founded as a Trust Authority by a number of leading commercial banks. Identrus has developed a rule book and technology standards to enable banks to issue digital certificates to their customers and accept digital certificates issued by other member banks.

The GTA and Identrus are complementary propositions. The GTA is primarily focussed on the B2C, B2A, C2A markets. The GTA has an 'open' policy regarding membership that is likely to permit other sectors to become GTA members in the future. The GTA is also 'open' in the mode of operation, so that the certificates issued under the GTA umbrella can be relied upon by all recipients, including those who do not have a business relationship with the GTA. The GTA has a cross validation policy that provides for the interaction between different PKI hierarchies.

Government Initiatives

Across the EU, governments are implementing initiatives to promote e-commerce in general and Internet applications and services in particular. The European Commission has been pro-active, as have a number of member governments. These initiatives promise to bring major parts of the public sector on-line over the coming years and will therefore require and encourage the use of trust infrastructures.

12. About digital signatures

To verify for example the identity of the sender of a document, authentication via digital signatures can be used. Digital signatures are based on public key cryptography, which works with a key pair comprised of a public key and a private key. The public key may be freely disseminated. The private key must be kept secret. Two basic characteristics of public key cryptography are:

- It is currently extremely difficult to obtain the private key from the public key. This is based on the assumption that factoring is difficult;
- Each key in the key pair performs the inverse function of the other. What one key does, only the other can undo.

To create or verify a digital signature, two complex mathematical equations, called the hash function and the signing function, are used. The hash function is a one-way transformation of a document into a fixed-sized string, which can be seen as the 'digital fingerprint' of the document. The signing function is the process of encrypting a document with the signer's private key. To create a digital signature, the sender signs the outcome of the hash function (called a message digest). The receiver of the digital signature applies the same hash-transformation to the document and then decrypts the message digest using the public key of the sender. If both outcomes are the same, the signature is successfully authenticated. If they are not, either someone is trying to impersonate the sender, the message has been altered since it was signed or an error occurred during transmission.

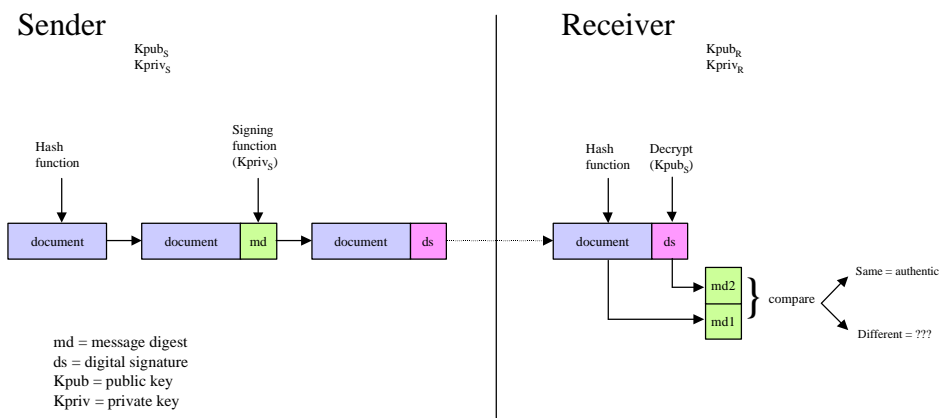


Figure: working of a digital signature

Besides these cryptographic calculations there is a need for a trusted entity (a Trusted Third Party) that guarantees the individual's identity and the relationship to the associated public key. The trusted entity that issues digital certificate to its subscribers, binding their identities to the key pairs they use to digitally sign electronic communications, is called a Certification Authority (CA). Certificates have a validity period, normally one or three years. Before the validity period ends, however, certificates can be revoked. For example, a certificate would be revoked if the private key is compromised. All issued certificates are stored in a Repository with a special area for the revoked certificates, called the Certificate Revocation List (CRL). Upon receiving a signed message, the relying party always needs to check the Repository. This complete infrastructure, based on public key cryptography, is called a Public Key Infrastructure (PKI).

An extensive explanation of PKI, digital signatures, cryptography, etc. can for example be found at <http://www.rsasecurity.com/rsalabs>

13. GTA Glossary

The following list explains the meaning of terms and abbreviations, frequently used within the GTA.

Term	Abbreviation	Meaning
Attribute Authority	AA	An entity trusted by one or more entities to create and assign attribute certificates. Note that a CA may also be an AA.
Attribute Certificate		A set of attributes which are bound to an entity by the signature of a trusted entity.
Authorised Relying Party	ARP	A relying party that is internal to the GTA infrastructure, i.e. it has a contractual relationship with an STA, covering certificate validation services. The ARP may or may not also hold a certificate, i.e. may or may not be a subscriber.
Authority Certificate		A certificate whose subject is a CA and whose associated private key is used to sign certificates.
Authority Revocation List	ARL	A CRL that only identifies revoked authority certificates and no end entity certificates. The GTA issues an ARL for the purpose of identifying revoked MTA certificates.
Certificate Policy	CP	<p>A named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements.</p> <p>The document, managed by a CA, describes among other things the manner in which Identity Certificates issued by the CA may be used and the obligations of the CA and the relevant End Entity in relation to such Identity Certificates.</p> <p>The Certificate Policy (or policies) under which a certificate is issued is indicated in the 'certificate policies' extension of the certificate.</p>
Certificate Revocation List	CRL	A digitally signed list issued by an STA to identify end entity certificates that have been revoked but have not expired yet.
Certificate Validation		The process of checking the revocation status of the certificate of a requesting party, either by comparing the certificate with its possible occurrence on a CRL/ARL or by sending an OCSP request to a Validation Authority.
Certification Authority	CA	An entity trusted by one or more entities to create, assign and revoke or hold public key certificates. In the GTA infrastructure all TAs are CAs.

Term	Abbreviation	Meaning
Certification Practice Statement	CPS	<p>A statement of the practices which a CA employs in issuing certificates.</p> <p>The GTA CPS describes the practices employed by the GTA to support its certification services to MTAs. A separate CPS is provided by each MTA, which describes the procedures, and practices carried out by that MTA in issuing certificates to its STAs. Similarly, each STA has its own CPS which describes the procedures and practices followed by that STA in issuing certificates to its end entities.</p> <p>To ensure a consistent level of trust, security and interoperability across the GTA hierarchy, the GTA sets minimum requirements, which all Trust Authorities (TAs) within the GTI must comply with. These are included in the GTA Rule Book.</p>
Cross certification		A process by which two CAs mutually certify each other's public keys and a particular CP in the first domain is considered by the authority of the first domain to be equivalent to a particular CP in the first domain.
Cross validation		The situation where an Authorised Relying Party under either an external PKI or the GTA structure is able to transparently validate certificates issued to end users under the auspices of both PKIs. Conversely, an end user with an ID certificate issued under the auspices of an external PKI or the GTA can be transparently accepted by an Authorised Relying Party under both structures.
End entity (End user)		A certificate subject that uses its private key for purposes other than signing certificates or an entity that is a relying party. The term end-user has the same meaning.
External Relying Party		A relying party that does not have a contractual relationship with any STA covering services for the validation of certificates.
Global Trust Authority	GTA	<p>An organisation which provides a global PKI framework.</p> <p>Global Trust Authority S.c.r.l. is a company incorporated in Belgium with its principal place of business at rue Marie Thérèse 11, 1000 Brussels.</p>
Global Trust Authority Infrastructure	GTI	The public key infrastructure established and maintained by GTA, consisting of at least the GTA, all MTAs and all STAs.
GTA Operational Authority	GOA	A management group established by the GTA Board for authorising the operations to be performed on the GTA Root.
GTA Policy Authority	GPA	The part of the GTA organisation that sets the policy rules of how the GTI will operate. The GTA Board will act as the policy authority for the GTA.
GTA Root Processor		The external entity that provides and manages the secure operation of the GTA Root, i.e. the party that is providing the outsource service for the GTA Root.
Identity Certificate	ID cert	A digital certificate that cryptographically binds a public key to the identity of the owner of the public key.
Master Trust Authority	MTA	A Trust Authority which exists at level 2 of the GTA hierarchy. MTAs are responsible for registering and certifying STAs.
OCSP Responder		An entity that provides OCSP responses.

Term	Abbreviation	Meaning
Online Certificate Status Protocol	OCSP	A protocol useful in determining the current status of a digital certificate, without requiring CRLs. OCSP provides more timely revocation information and may be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.
Policy Approval Authority	PAA	A management group that is responsible for authorising the use of particular certificate policies and certification practice statement(s) for a PKI. The overall PAA for the GTA infrastructure is the GTA Board. Each MTA and STA has its own PAA.
Public Key Certificate		The public key and identity of an entity together with some other information, rendered unforgeable by signing the certificate information with the private key of the certifying authority that issued that public key certificate.
Public Key Infrastructure	PKI	An infrastructure (consisting of software, hardware, procedures, personnel, documentation, etc.) that governs the use of public key cryptography.
Registration Authority	RA	An entity who is responsible for identification and authentication of subjects of certificates, but is not a CA or an AA and hence does not sign or issue certificates. A RA may assist in the certificate application process, revocation process, or both.
Relying Party	RP	An entity which accepts and relies on a certificate. Within the GTI, there are two types of relying parties: Authorised Relying Parties and External Relying Parties.
Root key		The public key used to validate the first certificate in the chain of certificates as a part of certification path processing, in this case the public key of the GTA.
Rule Book		A set of documents which sets out the various rules and requirements for parties participating in the GTA Infrastructure, parts of which are to be made available by the GTA to each MTA and parts of which are to be made available by each MTA to each of its STAs.
Scheme		A system that provides application services to its users based on PKI services via one or more STAs.
Scheme Trust Authority	STA	A role offering TA services to a particular scheme. STAs are responsible for issuing certificates to end-users.
Subscriber		An entity to which a certificate is issued (also known as the certificate subject).
Trust Authority	TA	An entity that can be relied on to implement GTA Infrastructure services and to uphold GTA Infrastructure requirements for security and risk management. This primarily consists of a certification authority but may include other roles such as registration authority, key recovery agent, etc. The GTA, MTA and STA are all TAs.
Validation Authority	VA	An independent role that keeps an on-line database for the validation of STAs and MTAs. Also used to denote an OCSP Responder.