Thales Gemalto Document Management System
Secure, scalable and modular life cycle management solution for your electronic documents
An ever increasing number of governments are making significant, long term investments in electronic Document (eDocument) programs. The main objectives are to:

- **increase security** - reduce fraud; make the roads safer; secure borders
- **offer new services to citizens** - speed reimbursements; increase online services while reducing operating costs

### Counting the cost of identity fraud
Identity fraud is the act of using a stolen identity to obtain goods or services by deception. This usually involves the use of stolen, forged or counterfeit documents such as a passport or driving license. The term ‘goods or services’ typically includes bank accounts, mortgages, credit cards, rail passes and job applications, or simply dishonest claims for state benefits.

The true cost of identity fraud is difficult to evaluate. However, it undoubtedly places a huge burden on wider society. In 2011, a study undertaken by the German Ministry of Interior revealed that the total cost to the nation of each forged document was €50,000.

### eID and eServices adoption
There is a growing trend towards large-scale adoption of electronic identity cards and electronic services.

The Boston Consulting Group has predicted that, in 2020, **30% of transactions will be digital**, enabling a $30-50 billion annual saving. In addition, according to research company Acuity Market Intelligence report of March 2017, the number of electronic national ID cards in circulation will reach 3.6 billion by 2021.

This digitalization implies a **very high level of trust** in the security of the infrastructure that is responsible for issuing and managing the eDocument.

Identity programs are a long term investment
Identity programs represent a major, long term investment for government. Programs can last ten years and, over this period, regulations and technology will evolve. To maximize the return on investment in their identity programs, governments will seek solutions that not only deliver the highest level of security to reduce the cost of fraud, but also provide a **dynamic eID** that can evolve over its lifetime.

### Multi-application documents
More and more electronic documents, and in particular identity documents, are multiapplicative.

Thus there is a clear need to manage effectively all the applications within the document. This includes not just the release and content of initial applications, and updates when the ID evolves, but also the introduction of completely new applications once the document is in the hands of citizens.
The Gemalto Document Management System is a central solution at the heart of the issuance ecosystem

The Gemalto Document Management System (DMS) plays a central role in the issuance process - managing the eDocument and its applications to secure its issuance and enable usage.

The DMS interfaces with a range of back-end systems, such as a National Registry, Certificate Authority and the Interpol database, to retrieve or provide information. It also interfaces with main issuance systems, such as personalization centers in either centralized or decentralized issuance schemes, document delivery solutions, and post-issuance systems responsible for updating the eDocument.

The DMS solution architecture is inherently modular and highly scalable. It is made up of several system components, divided into three main categories:

- **Services**
  There are five services hosted on the DMS server: life cycle, issuance, consultation, SMS notification, and application management. All these services are totally independent and can be deployed at different times.

- **Client interfaces**
  The DMS offers client interfaces for supervisors and other authorized personnel, in order to administrate and supervise the system.

The Gemalto Document Management System (DMS) offers government bodies a field proven and scalable solution for the secure issue and use of eDocuments such as national eIDs, ePassports, eDriving Licenses and eHealth cards, thereby helping them to protect their investments.
Web applications

The DMS works with web applications hosted on web servers. Web applications are used at key stages of the eDocument life cycle. At delivery, authorized personnel will register all eDocuments received and all eDocuments issued to citizens.

If an eDocument is lost or stolen, a dedicated web interface is accessible to record the event. If information on an eDocument needs to be checked, authorized personnel can consult the document history and status via a dedicated web application.

DMS services overview

Life cycle services
This is the key role of the DMS. It manages the life cycle of the eDocument, whether it is a passport, an eID, a driving license or a healthcare card. It also manages the life cycles of the applications hosted in the eDocument, and the eCertificates. The flexibility is such that the life cycle of each entity can be customized in line with project requirements.

Issuance services
The DMS supports services that manage the issuance of an eDocument. The DMS will receive the issuance request, check data and prepare every application to be hosted in the eDocument. In addition, it will manage all personalization centers, whether in a centralized or decentralized scheme.

Consultation services
The DMS offers the opportunity to check eDocument history and status. This control can be performed in a number of different ways: online through a connected terminal used by an authorized member of staff, or offline in the field using a mobile terminal with blacklisted eDocuments uploaded from the DMS.

SMS notification services
This enables citizens to be notified throughout the eDocument's life cycle. For example, the citizen can be advised that the document has been delivered and is ready for collection. He or she can also be notified that their eID is due to expire, and that the renewal process should be launched.

Application management services
Application management is critical. A growing number of eDocuments host several applications, and several releases of an application may be deployed over its life cycle. Furthermore, new applications can be loaded once the eDocument has been issued. The services offered by the DMS will manage effectively all eDocument applications, encompassing life cycles, the generation of updates for existing applications, and the preparation of new applications for upload to the eDocument.
Easy integration with external systems

To communicate with external systems, the DMS uses connector and gateway modules. These are pluggable components implementing a predefined interface dedicated to a specific system that can implement different technologies:

- Secure web service (SOAP, REST)
- Queue messaging
- File Transfer Protocol

Best-in-class security

As a central and key element in the eDocument issuance scheme, the DMS will implement different security mechanisms to ensure the confidentiality and integrity of eDocument applications and data.

Encrypted communication

All communication between the DMS and internal systems (KMS, DS, DMSR web application, DMS client) or external systems (CA, personalization centers, National Registry) employs secure protocols such as HTTPS and FTPS.

Issuing request identification

The DMS validates the origin and the integrity of each issuance request it receives. Proof of origin and integrity are guaranteed by digital signature. Each issuance request is digitally signed by the issuing systems before being processed by the DMS.
Database encryption
The Gemalto DMS database stores sensitive information about the document content, status and history. It may also store the document holder’s personal data. This Personally Identifiable Information (PII) is extremely sensitive and its confidentiality must be ensured to comply with privacy laws and regulation. For that purpose, the DMS database is encrypted, with secret information stored securely in a certified Hardware Security Module (HSM).

File encryption
The Gemalto DMS offers the potential to encrypt all files managed by the system: audit files, log files, production files.

Applicative encryption
The Gemalto DMS can implement end to end data encryption. The data encryption is performed by an HSM-based solution that encrypts all sensitive data before storage in the DMS database and decrypts all data when processing it. This encryption method protects against insider attacks.

User management
The Gemalto DMS only provides access to authenticated users. The user authentication is performed by verification of the username and password stored in a LDAP or LDAPS (Secure LDAP) system. A minimum of four different user roles can be defined: operators, administrators, supervisors and auditors. If necessary, it is possible to create more user roles. Any single feature or set of features of the Gemalto DMS can be associated with a specific, newly created role.

Key benefits
The Gemalto DMS delivers unique benefits:

Reduce significantly fraud on eDocuments
The Gemalto DMS offers multi modal eDocument consultation services via fixed stations, or using mobile terminals uploaded with eDocument blacklists that will help police workforces to systematically proceed with eDocument status verification before proceeding with identity verification. This will help to improve significantly the lost/stolen capture rate.

Start small and scale fast for an optimized return on investment
The Gemalto DMS is designed to be inherently modular and highly scalable, enabling government to quickly deploy the necessary features and services and to scale the system with new services depending on future needs.

Ensure citizen data security
The security and protection of citizen data are fundamental for any government when issuing eDocuments. The increasing deployment and usage of online services give even more value to the citizen’s digital identity. Thales has implemented all its know-how and expertise in digital security.

Easy integration
Gemalto DMS integration in any ecosystem is largely facilitated by the use of web service connectors and gateways to integrate with external systems and via platform interoperability to PKI systems.

Technical data

**Supported standards**
- Global Platform™/JavaCard™
- Multos™
- ICAO Doc 9303
- TR0310
- PIV / FIPS 201
- ISO/IEC 19794
- PKCS
- HSM FIPS 140-2 Level 3
- BS 7799 / ISO 17799 / ISO 27001

**Supported applications**
- ICAO
- IAS
- Biometric matcher
- EU Digital tacho
- EU driving License
- MPCOS

**Supported infrastructures**
- OS: Windows, Linux [On Demand]
- Application server: Widlly, websphere (On demand)
- Database: Oracle, Microsoft SQL
- Browser: Chrome, Firefox, IE, Safari
- HSM: Safenet, Thales

**Supported PKI**
- Microsoft CA
- Multicert
- Opentrust
- PrimeKey
Examples of customer implementations

**ALGERIA eHealthcare**
A complete eHealthcare solution for Algeria

Algeria is a fast-growing country with a population of close to 40 million, over 80% of whom benefit from the national healthcare organization, the Caisse Nationale des Assurances Sociales des Travailleurs Salarisés (CNAS).

As prime contractor, Thales managed the entire project, including delivery of a complete Secure Issuance Solution, incorporating a Document Management System and a personalization solution configured for a high-volume centralized personalization environment and color photo printing by dye sublimation technique.

Leveraging its solutions expertise, Thales assisted the CNAS in launching the production process and ensuring proper training for the CNAS personnel.

**CAMEROON eID**
Cameroon’s new national identity card program: much more than an ID

Launched in 2016, Cameroon’s new national identity card and the complete overhaul of its system of identification and card manufacture for new documents are an illustration of the determination of the country’s authorities to strengthen homeland security, in particular by combating identity theft and document fraud.

The national identity card is produced alongside other documents such as resident permits, refugee cards, professional ID cards for personnel of the General Delegation for National Security, retirement cards for public servants who worked in national security, with possibilities for extension to other public or private government bodies.

Cameroon is at the same time modernizing its solution for the enrollment of citizens. Authorities opted for Thales’ Gemalto Enrollment platform, its Document Management System and its card personalization with secure issuance software to implement color laser engraving technology.

**OMAN ePASSPORT**
On January 15 2015, Royal Oman Police (ROP) launched the new Omani electronic passport.

The new ePassport design is derived from Omani heritage, including the dagger and Islamic and Arabic decorations as well as three dimensional drawings of the most prominent landmarks of Oman.

The new document incorporates a microcontroller containing the holder’s information, including biometric identity, a digital image and electronic signature.

Thales is proudly providing the Royal Oman Police with an end-to-end electronic passport solution for the Sultanate. The turnkey solution encompasses Thales’ ICAO* compliant ePassport documents, and a full software solution suite to enroll citizens, and personalize and manage the life cycle of secure documents.

**Features of the RSA eID:**

In addition, Thales provided 12 million Health Insurance Cards, which securely identify each beneficiary and their dependents, as well as enrollment and eGovernment solutions.

The tailor-made Thales solution includes consulting services and training, card issuance and personalization, card acceptance secured by PIN codes for patients and USB keys for health professionals, and a PC-based application to manage claim and prescription functionality.

The 700 million e-prescription landmark was reached in May 2016.
Why Thales?

Thales is a reliable and trusted partner for all your public sector ID initiatives including ePassports, eVisas and other international and national identification schemes as well as healthcare and social security programs.

We offer a complete range of secure solutions that are tailored to local markets, and we deliver what you want, where you want it, with the support of a strong network of local partners.

Thales relies on 100 years of innovation in secure documents, and our unique expertise in digital security means we provide innovative, trusted solutions that you can count on.

- Our Gemalto Secure Documents offer physical, visual and electronic security for travel documents, eIDs and eVisas. These innovative products are designed with durability and security in mind. With over 10 FIPS certificates and 50 Common Criteria certificates we meet the most stringent international certification for highly secure applications.

- Our Gemalto Secure Solutions - such as Issuance - are designed to be YOUR turn-key solution, integrating state of the art security. They are evolutionary and serviced by local support teams.

- And because we know the success of your project does not rely on products and solutions alone, we offer our Managed Services - a complete range of services for governments, ministries, agencies and more ... In particular, Gemalto Issuance Managed Services offer you outsourced personalization services for all your secure documents, as well as mainstream services for your backup, contingency or disaster recovery plans.

Thales in brief

In the civil identity sector, Thales provides secure documents, robust identity solutions and services that address government programs for ID management and road safety, government digital identity infrastructures for trusted eServices, and border and visa management requirements.

Thales also addresses public safety and law enforcement challenges, offering best-in-class forensic solutions.

The company’s products and solutions are deployed in over 200 active programs worldwide, with specific expertise in secure document issuance, biometrics, document readers, authentication, ID management and data protection.

Thales collaborates with its clients to report and share best practices.