



gemalto explains

**Trusted Service
Manager**

**How to manage
end-to-end
security**

gemalto^{*}
security to be free

www.gemalto.com/digitalsecurity

The complexity of managing end-to-end security

1

The Key Ceremony

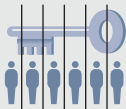
A one-time process that enables **key management**.

Banks and Gemalto can set up keys to securely exchange other keys and data packages.



Bank HSM

The keys are produced and encrypted inside the HSM* (Hardware Security Module).



Different parts of the keys are managed by different people.



At every stage of the process many secret keys are used to transport data securely between the bank and Gemalto.

An encrypted data file is produced. This secure package is sent to Gemalto.

2

The Key Ceremony is mirrored at Gemalto

A data processing engine unpacks secure files from the banks using the Gemalto HSM.



Gemalto HSM

The keys are decrypted and reassembled inside the HSM.



Like the banks, Gemalto has **key custodians** who manage different parts of these keys.

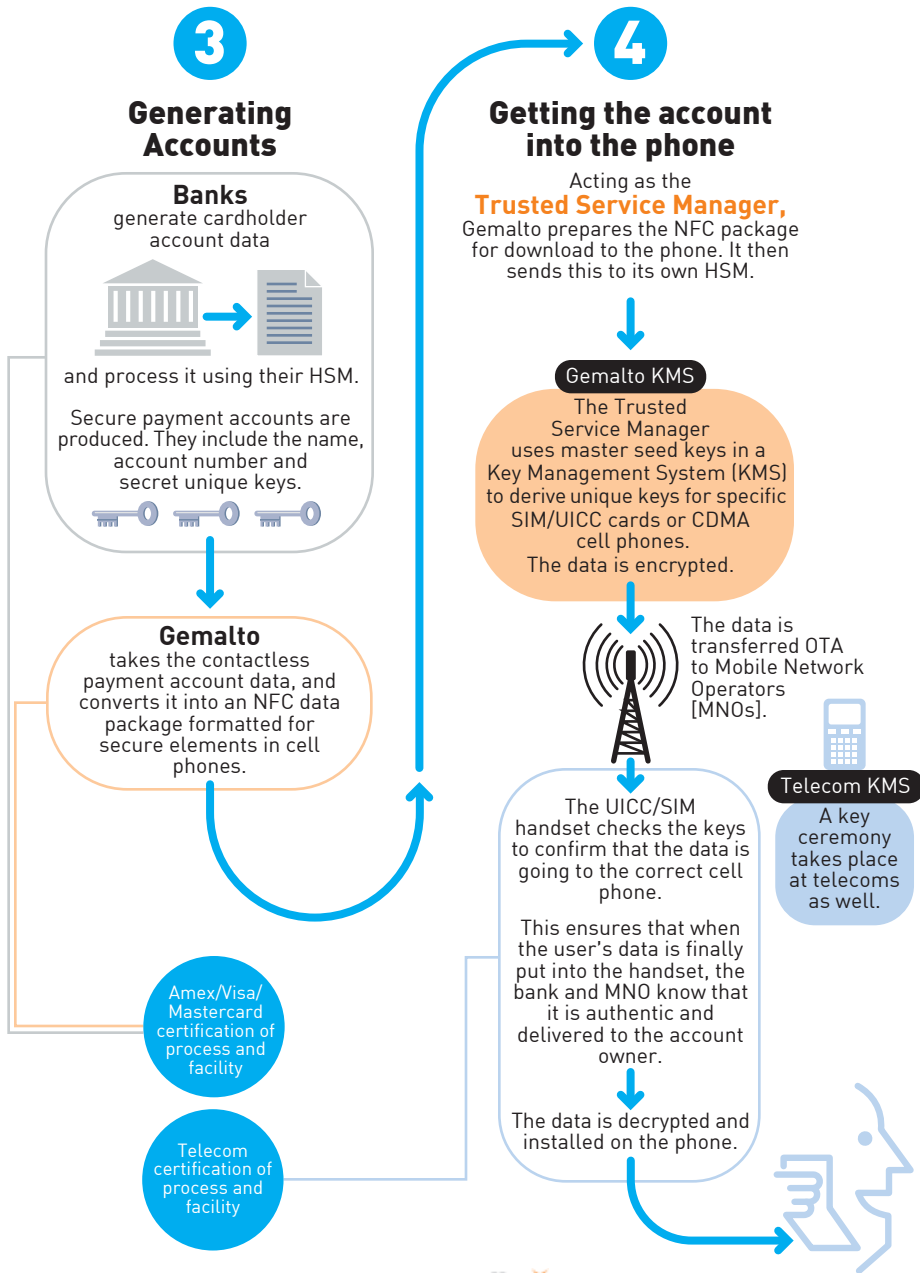


Different secret keys transport data securely at every stage of Gemalto's internal process.

Now data can be securely sent back and forth between Gemalto and the banks via the Internet.

*The Hardware Security Module is a hardware-based security device that generates, stores and protects cryptographic keys.

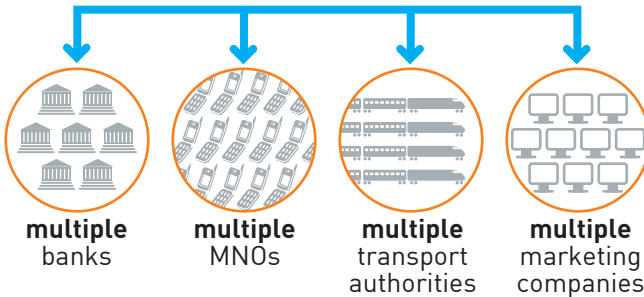
Banks and Mobile Network Operators need a go-between: a **Trusted Service Manager** (TSM). That's where **Gemalto** comes in.



BENEFITS

- **The Gemalto TSM** process ensures end-to-end security encryption between banks and SIM/UICC cards and CDMA cell phones.
- The data only works on the right phone.
- The encrypted data package cannot be used if intercepted.
- Can be securely loaded OTA.
- No human ever sees any account data, numbers or keys, and no machine sees them in the clear outside the HSM.

The TSM is a **bridge** between...



...and the **TSM** manages the payment account throughout its life cycle

What's an NFC Secure Element?

A smart card chip that stores information, manages security and provides a firewall between NFC applications and other elements in the phone.

It is installed in one of three ways:

1 SIM/UICC cards

2 micro SD cards

Cards are removable

3 Embedded chip

Chip wired into phone

gemalto
security to be free

www.gemalto.com/digitalsecurity