Security by Design,

A WINNING STRATEGY TO FACILITATE YOUR BUSINESS WITH MAJOR BANKS

Peter Winkelmans - Cyber Security Consulting Director

Your customer is a bank!

What does this mean?

- Bank have to fulfil on lot's of **requirements**
  - Capital requirements
  - Reserve requirements
  - Corporate governance
  - Financial reporting
  - Credit rating
  - …

Bank have to be compliant with lot's of **regulations**

- PCI DSS
- GDPR
- Basel II
- SOX
- ISO 27001
- …

So, the financial institution expects that:

Your solution is **compliant** with the **requirements and regulations of a financial institutions.**

Your organisation has the **same level of security maturity** as required for a financial institution.

When to implement these security requirements?

Design Principles

Security Concepts

Core Concepts

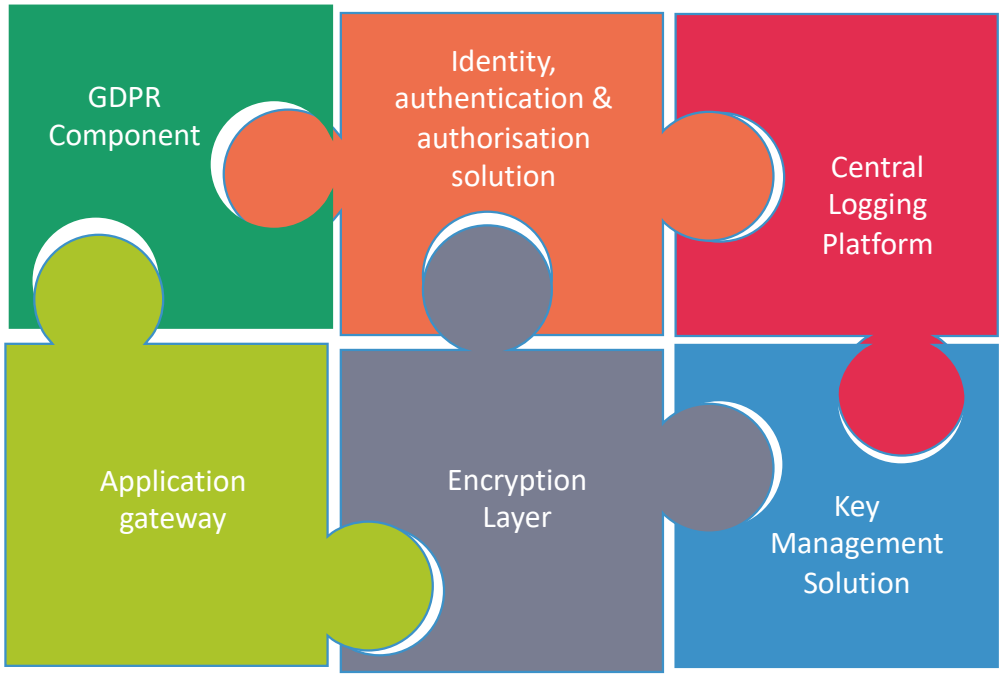
- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accountability
- Non-repudiation

10 Design Principles

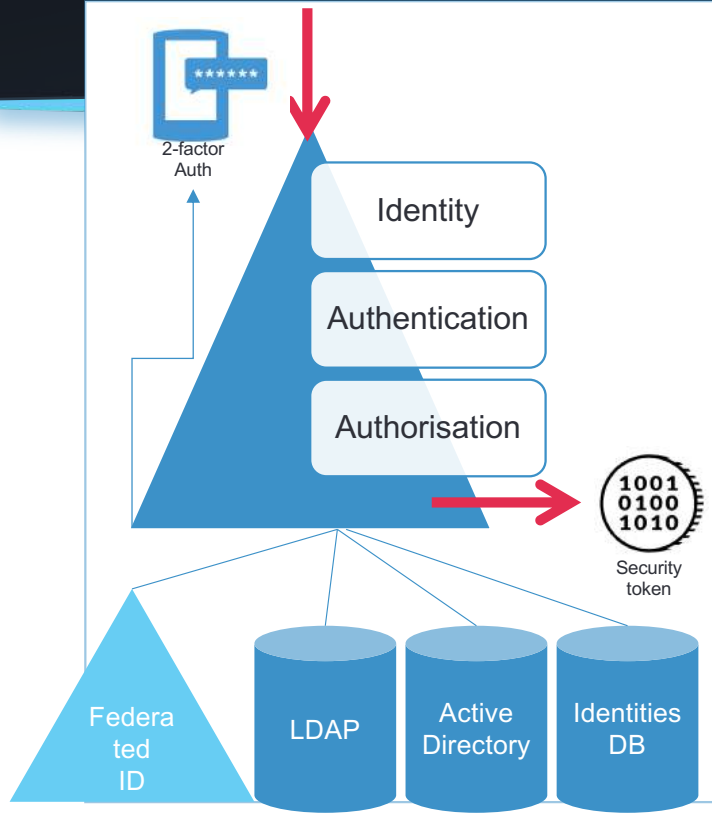
1. Minimise attack surface area
2. Establish secure defaults
3. The principle of least privilege
4. The principle of Defence in depth
5. Fail securely
6. Don’t trust services & Infrastructure
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

Design a security platform

Combine the right components



Identity and Access Management solution



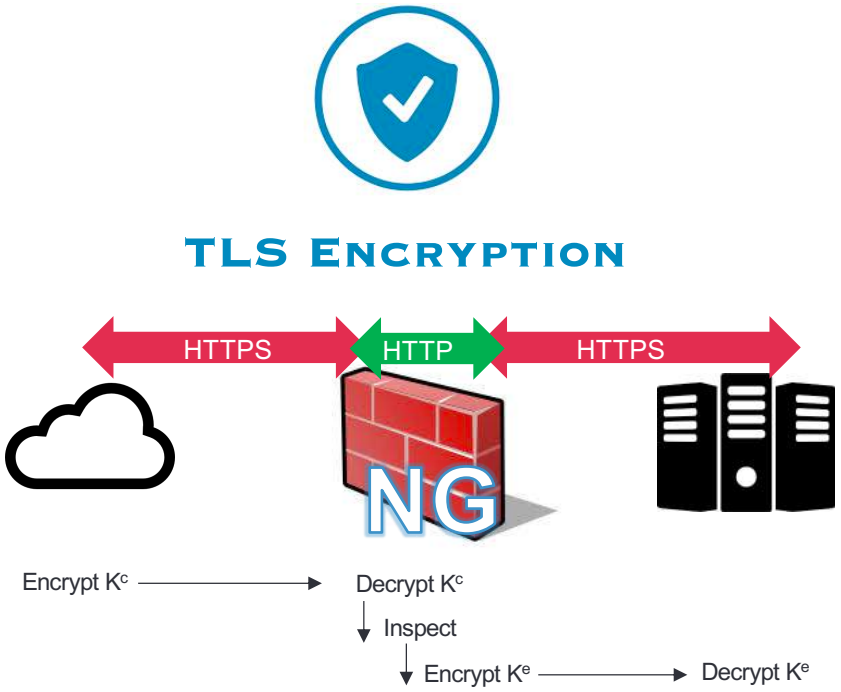
- **1 identification and authentication solution** (employees, customers, suppliers, …)

But it can have multiple sources

  - Active Directory
  - Database
  - Federated Identity

- Speaks all standard protocols (OpenID, SAML, OAuth, …)
- Multi-factor authentication ready
- **A database of identities is not your customer's database**
- Develop internal SDK , code snippets,…

Communication encryption



- **Https** is the default protocol
- For **external** and **Internal** communication
  - To protect your data flows.
  - To protect your authentication information (login and password, session ID's)

- **SSL Inspection**
  - Every SSL/TLS connection have to be inspected on the firewall or the proxy.

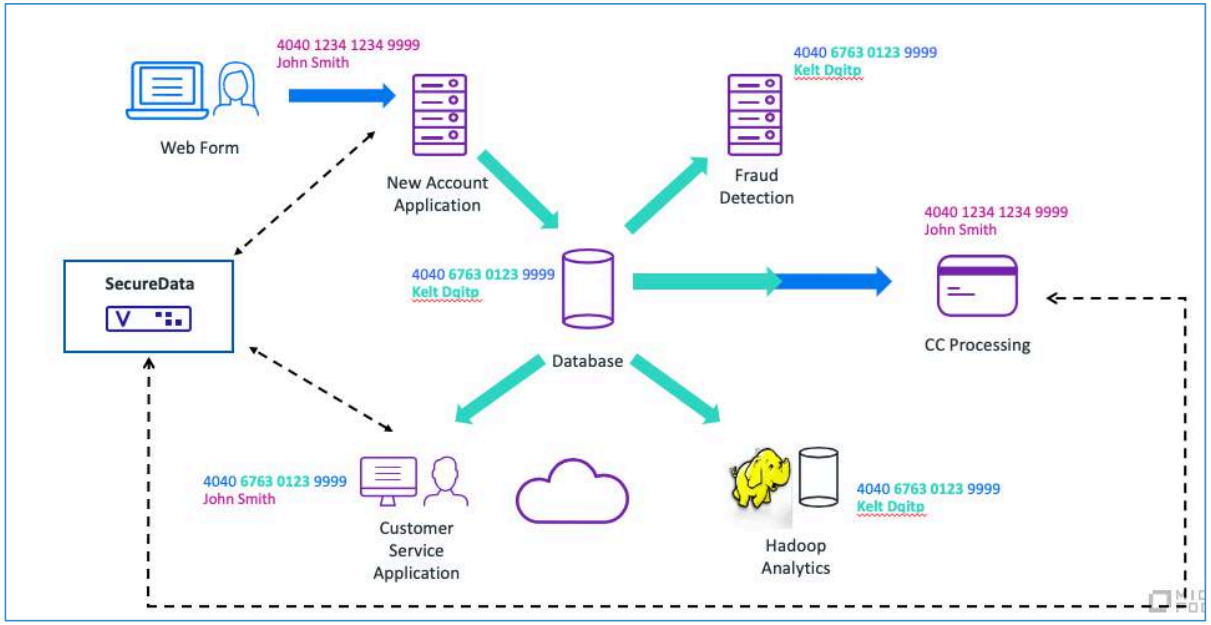
Data Encryption

Format-Preserving Encryption, Format-Preserving Hashing and Secure Stateless Tokenization

	Credit card	Name	Email	DOB
Original	1234 5678 8765 4321	Kylian Mbappe	Kylian.Mbappe@voltage.fr	31-07-1966
Standard AES-CBC	Ija&3k24kQotugDF2390^3232h	0OWioNu2(*872weW	Oiuqwriuweuwr%oIUOw1$dhs7j2jdds	8juYE%UkFa2345^WFLE
FPE AES-FFX	1234 5633 4678 4321	Sokr Sejzvp	rdadan.etmjpl@jqvevkn.pk	20-05-1972

- Supports virtually any data types in any format: name, address, dates, numbers, etc.
- Preserves referential integrity
- Only applications that need the original value need change
- NIST-standard using FF1 AES Encryption

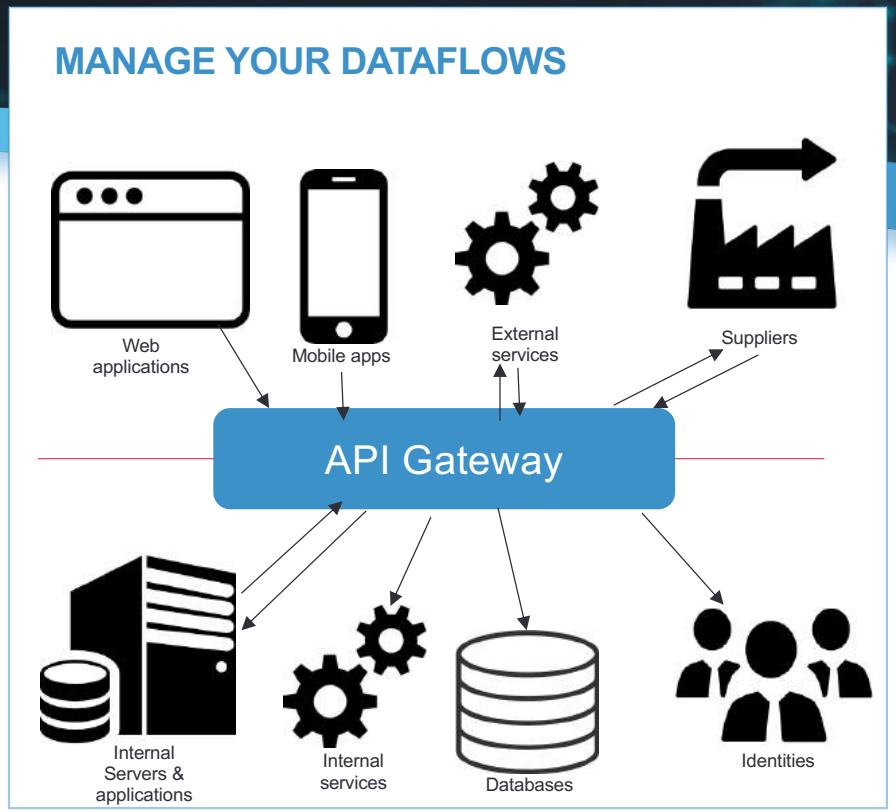
End-to-End data encryption



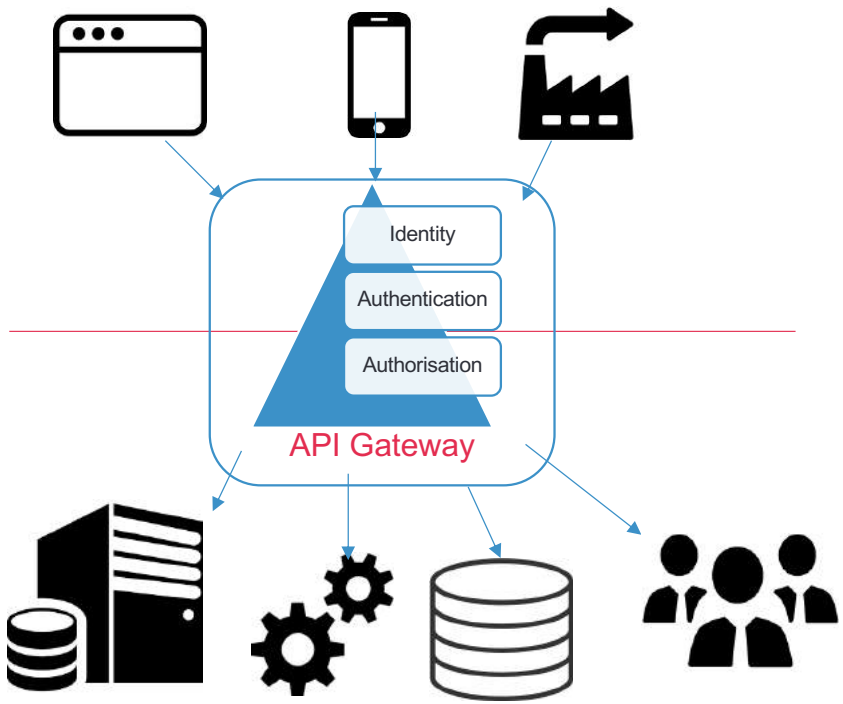
- Based on application identification and authorization
  - Only those applications get the decryption key
- Data decryption will be policy based.
  - Some applications see real data
  - Other applications see encrypted data
- Location of data will less important
  - (Cloud or on-premise)
- Secure non-production data
  - Your development, test and Q&A DB can be a copy of your production

API Management

Which one you choose?



API Gateway regulates access to your data & services

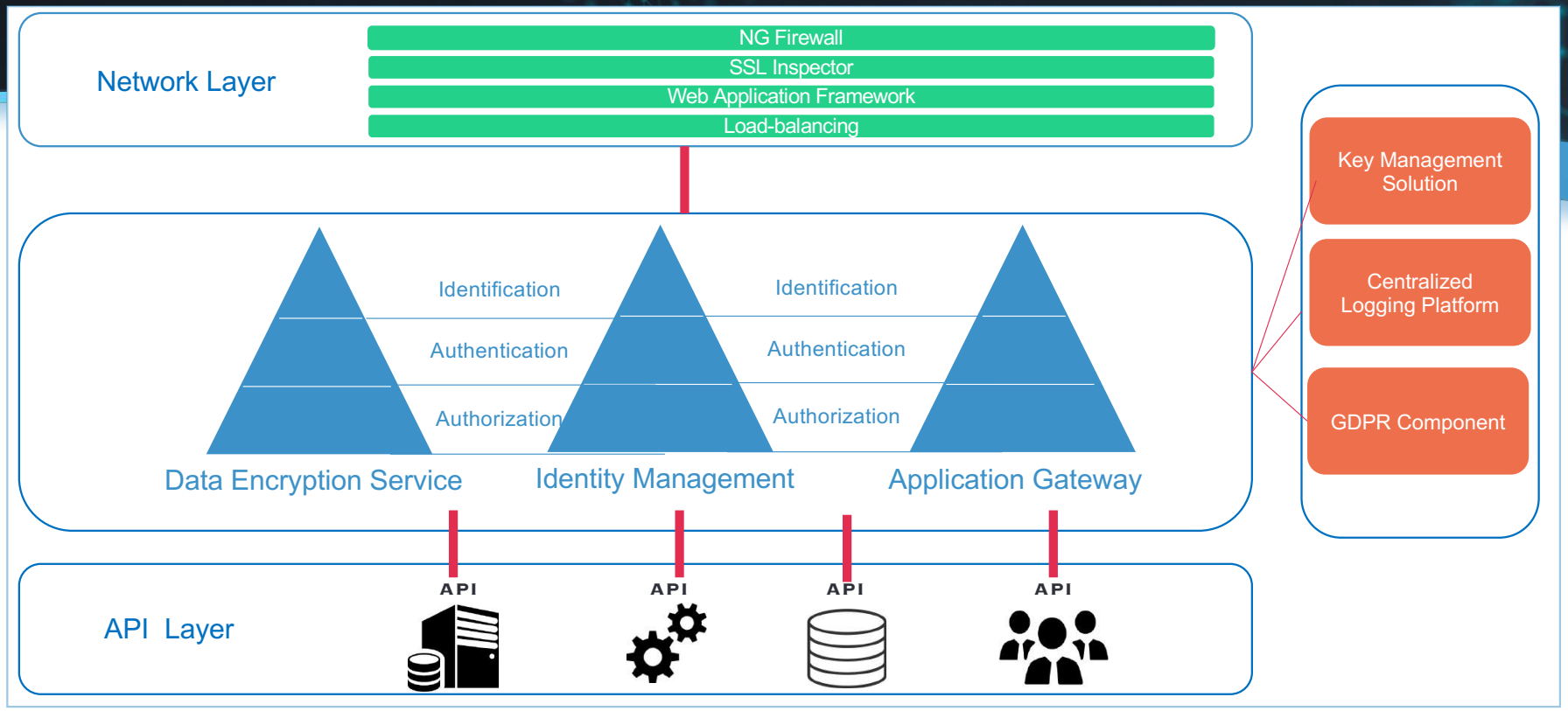


API GATEWAY

- API - development
  - Develop API as minimalistic as possible
- API Gateway
  - Identification and Authentication of your API-customers (API – Keys or certificates)
  - Authorisation to the different API's
    - Which application can use which data
  - Extra security functionalities

Global Security Platform

The combined components



Last but not least

Train
your
Developers
in
Secure Coding

Questions

?