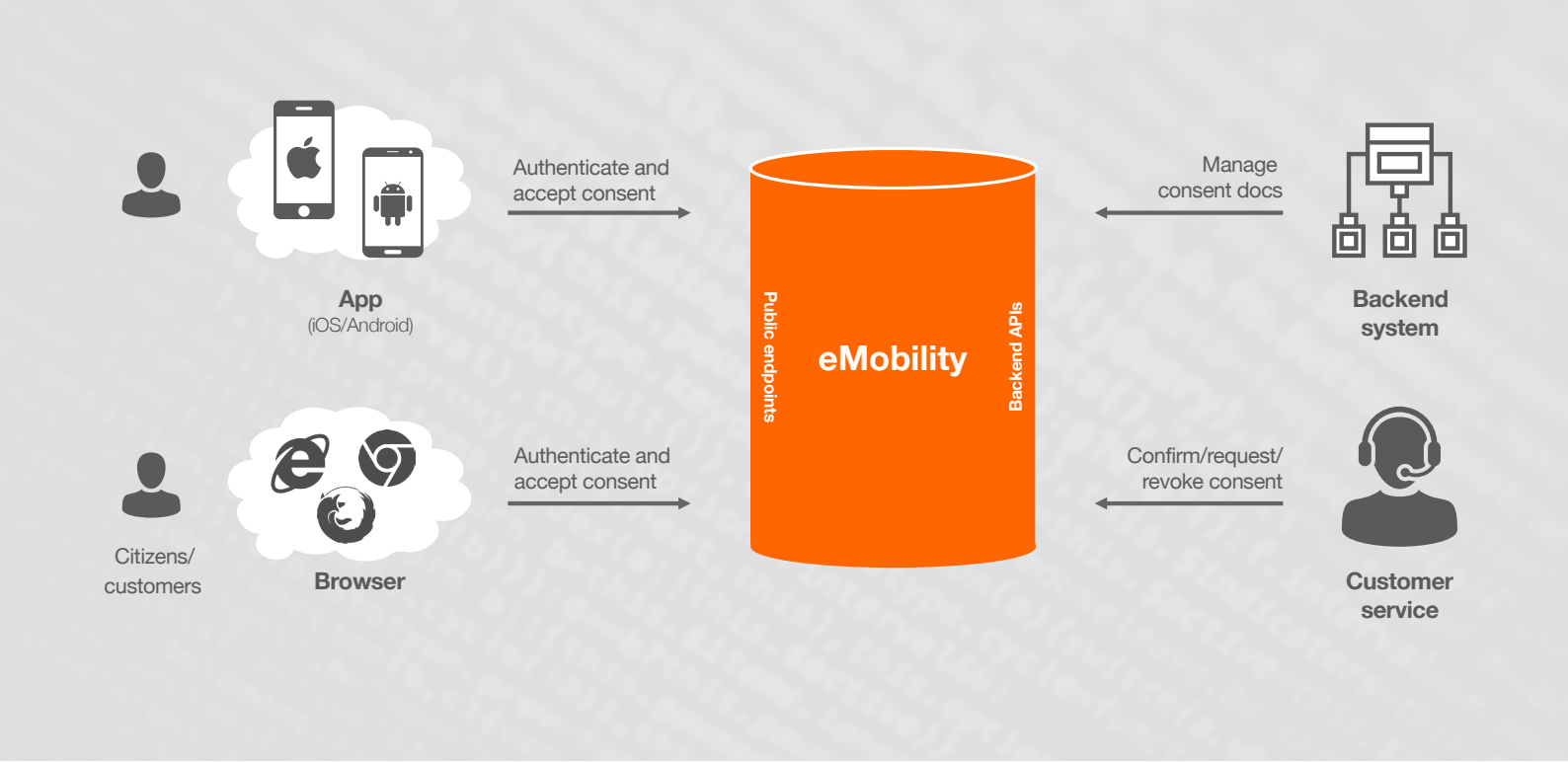
TRIFORK eMOBILITY

GDPR compliant Consent Management made simple



The Challenge

- EU General Data Protection Regulation will be enforced from May 25, 2018
- GDPR requires that valid consent must be explicit for data collected and the purposes that the data is used for
- This can be handled manually via a customer care team or similar

The Solution

- Trifork recommends central storage and administration of all user consents
- This recommendation ensures a swift and consistent turnaround and provides a better platform for the development of your business
- Trifork provides a solution based on an existing product, Trifork eMobility, that integrates via API's into your applications and infrastructure

Consent Management Overview

- Repository of all current & historic consent documents
- Multiple consent types and versions can be stored
- Consents are parameterised, meaning they reflect if the user checks different options
- Consent can be registered with multiple user ID's (email, phone number, NemID and more)
- Backend systems can enquire accepted consents for users
- All consents for specific users can be listed (data insight for a user)
- All consents for a specific user can be deleted upon request ("the right to be forgotten")
- Retention period can be configured

For more information, please contact Peter Flintholm
at **pfs@trifork.com**

TRIFORK
...think software

TRIFORK EMOBILITY

Mobile Login Solution

The Trifork eMobility product suite includes a simple Identity Provider developed specifically for user friendly and secure mobile logins.

The security model in a non-mobile enterprise is rarely suitable for mobile app use. Often they assume that the user is on a PC browser. When these services are used by mobile apps, the security architecture must be reconsidered, and often changed to accommodate the needs in a mobile environment.

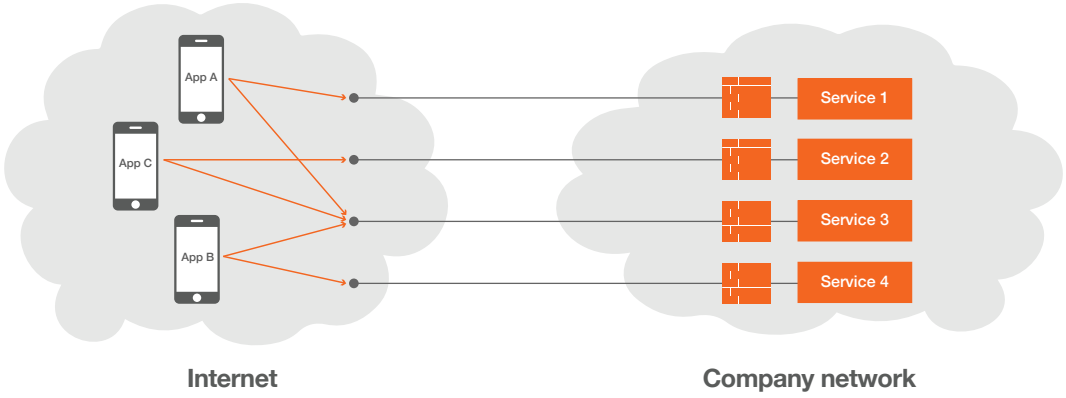
The eMobility Identity Provider makes it possible to develop mobile apps that access sensitive data in a highly secure way while also providing the easy-of-use that is expected in mobile apps.

Users can self-enroll on their device and subsequently make user friendly logins using pin/password or fingerprint. The solution allows for very flexible integration and UI customisation to match the app design.

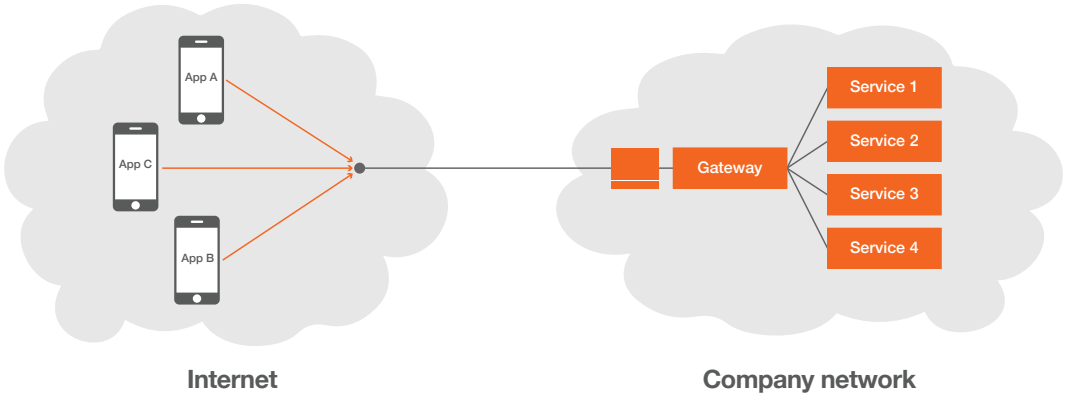
API Gateway

Also included in eMobility is a simple API gateway which we call SSG for Secure Service Gateway. The SSG will validate JWT tokens issued from the Identity Provider and proxy requests to the allowed internal services. It is not a requirement to use the SSG when using the eMobility Identity Provider – any other API gateway can easily be used as well.

The SSG is stateless and hence provides a solution that will scale to any throughput requirements.



Challenge with multiple clients accessing backend services



Trifork eMobility simplifies access and authentication

For more information, please contact Peter Flintholm
at **pfs@trifork.com**

TRIFORK
...think software