cocoon DATA

# SafeShare

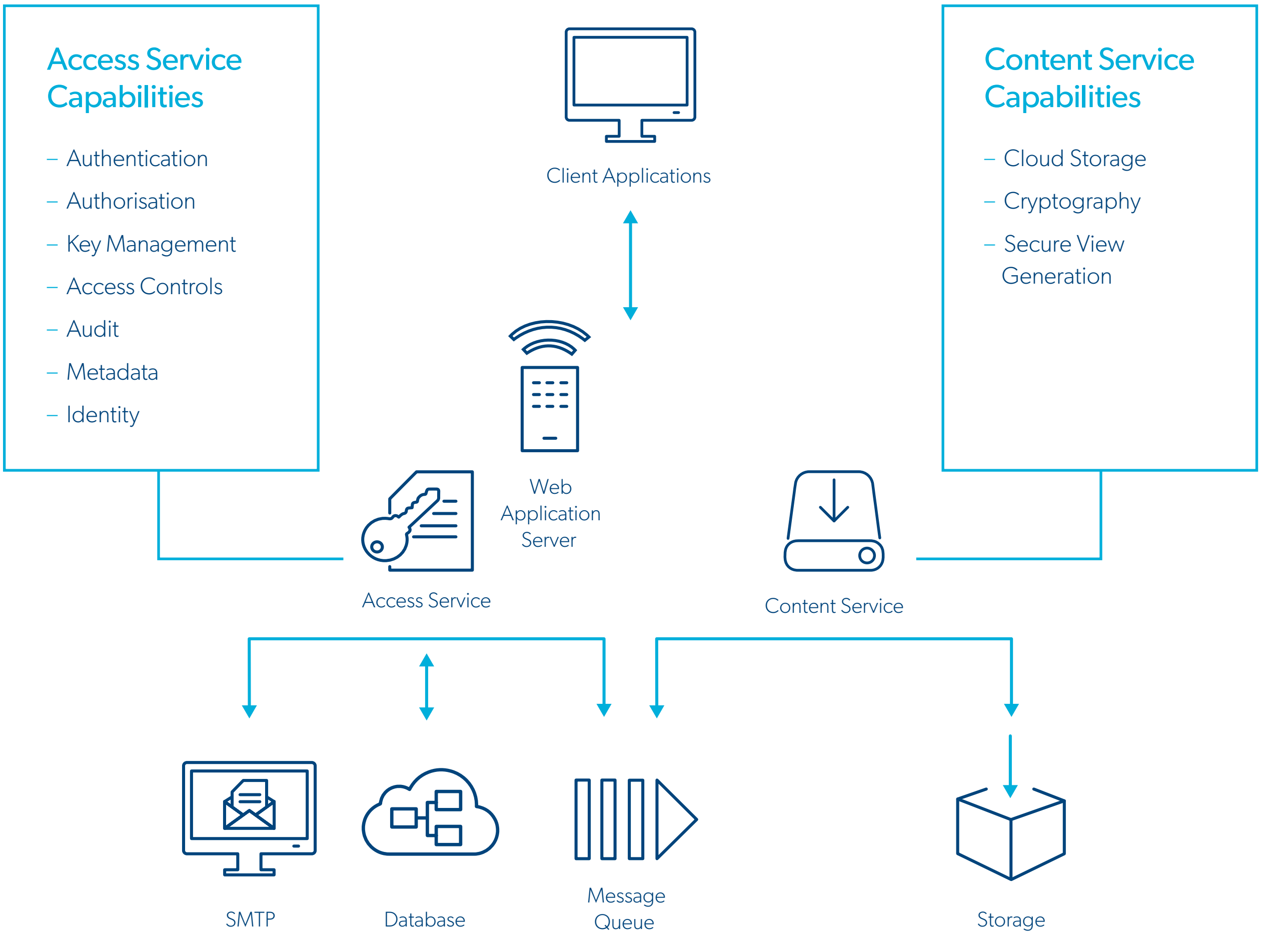
## Technical Specifications

# Overview

Cocoon Data SafeShare is a highly secure file sharing application. It is part of Cocoon Data's data security platform (dsp) that enables enterprise and government to discover, protect and control sensitive information, whilst transferring and sharing it safely with both internal and external stakeholders.

SafeShare enables any file to be uploaded, encrypted, stored and securely shared by internal and external users. Before sharing, the owner of the data (the 'originator') can apply sophisticated access controls over who has access, when they have access and how they can consume the data. SafeShare provides detailed audit tracking into who, when and how all information has been accessed (by 'collaborators' and 'viewers').

## SafeShare Components



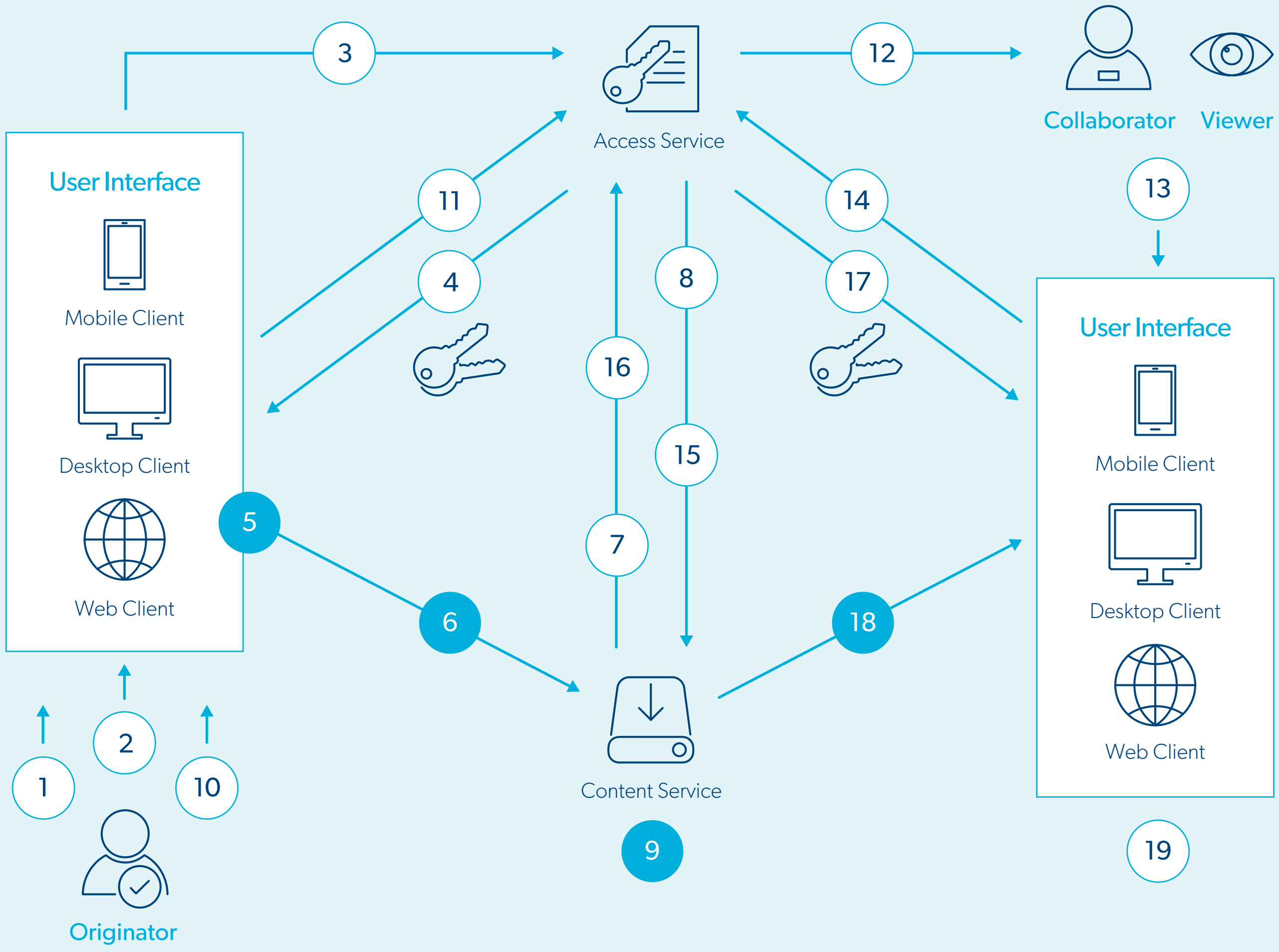
### Access Service Capabilities

- Authentication
- Authorisation
- Key Management
- Access Controls
- Audit
- Metadata
- Identity

### Content Service Capabilities

- Cloud Storage
- Cryptography
- Secure View Generation

## SafeShare Example Process Flow



### Originator

Uploads a file (which is secured through encryption) and sets access controls so file can be safely shared both internally and externally.

### Collaborator

Accesses content to comment, edit and share.

### Viewer

Accesses content but is restricted to view only.

### Originator: Document Upload

1. User (Originator) is authenticated
2. Upload file to SafeShare
3. User Interface requests keys from Access Service
4. Keys sent to User Interface
5. File encrypted at User Interface
6. Encrypted file and file token sent to Content Service
7. Content Service requests file token validation with Access Service
8. Access Service acknowledges file token validity
9. Content Service securely stores document

### Originator: Document Upload

10. User (Originator) shares file with other user(s)
11. User Interface sends share request to Access Service
12. Access Service notifies user(s) by email that a file has been shared
13. User (Collaborator) clicks on the link in the email and authenticates with User Interface
14. User Interface sends file token and requests keys from Access Service
15. Access Service requests file token validation with Content Service
16. Content Service acknowledges file token validity
17. Keys sent to User Interface
18. Encrypted file sent to User Interface
19. File downloaded and decrypted at User Interface

KEY: X Encrypted file

# Technical Synopsis

## Authentication and Authorisation

- SafeShare is OAuth2.0 compliant
- Username and password authentication
- Two-factor authentication

## Cryptography

- Advanced Encryption Standard with 256-bit key sizes (AES-256) for encryption and decryption
- Protection to the endpoint via browser based encryption
- Large data set encryption quality assured via Cipher BlockChaining (CBC) and incorporating Public-Key Cryptography Standards (PKCS) #7 padding
- Content verification by hashing with SHA-512 which has equivalent security to AES-256

## Multi-Tenancy

- Multiple organisations hosted within the same deployment and on the same infrastructure
- User can only access data within the organisations to which they have been granted access

## Access Controls

- Fine gradient access controls for view, inline edit, download, create, manage and co-own
- Fail-safe security principles incorporated throughout the system – permission is denied unless explicitly granted

## Key Management

- AES-256 keys and initialisation vectors used for cryptography
- Cryptographic keys are generated by secure pseudo random number generator algorithm, SHA1-PRNG, from the IEEE P1363 standard
- New key for every document and every version of a new document

# Support and Deployment

## File Types

- Any file types for upload, including: Microsoft Office / Adobe / Multimedia, including video and MPX
- 35+ types of file for viewing
- Any file size

## Devices

- Web client available on popular browsers (up-to-date versions of Chrome, Firefox, Edge and Safari)
- Desktop client applications (Windows)
- Android and iOS mobile devices

## Infrastructure

- Public
- Private
- On-premises
- SaaS via Openstack
- AWS
- Azure

## Platform

- Ubuntu 64 bit: V14.04 LTS
- Red Hat Enterprise Linux 64 bit: V6, V7
- CentOS 64 bit: V6, V7
- OpenJDK: V8
- RabbitMQ: 3.5.6
- PostgreSQL: 9

# About Cocoon Data

Cocoon Data is a global technology brand, that provides data-centric security solutions for enterprise, government and citizens. Our easy to use security platform will discover and identify your sensitive information and where it resides, protect and manage your risk by sharing and storing your sensitive data securely, and implement controls to restrict when and how users access your data. Then monitor and analyse user activity.

We ensure security is never an afterthought, protecting information at a data-level from the start, and at every point of its journey. Safe and efficient sharing of data across internal and external stakeholders, devices, networks and geographic regions is enabled and encouraged. You have total control, visibility and auditability of your sensitive information.

Contact us at **info@cocoondata.com**

**cocoondata.com**

COCOON DATA