VOTING Stimmregister

Transport Security

Author	Abraxas Informatik AG
Classification	public
Version	1.1
Date	31. Jan 2024

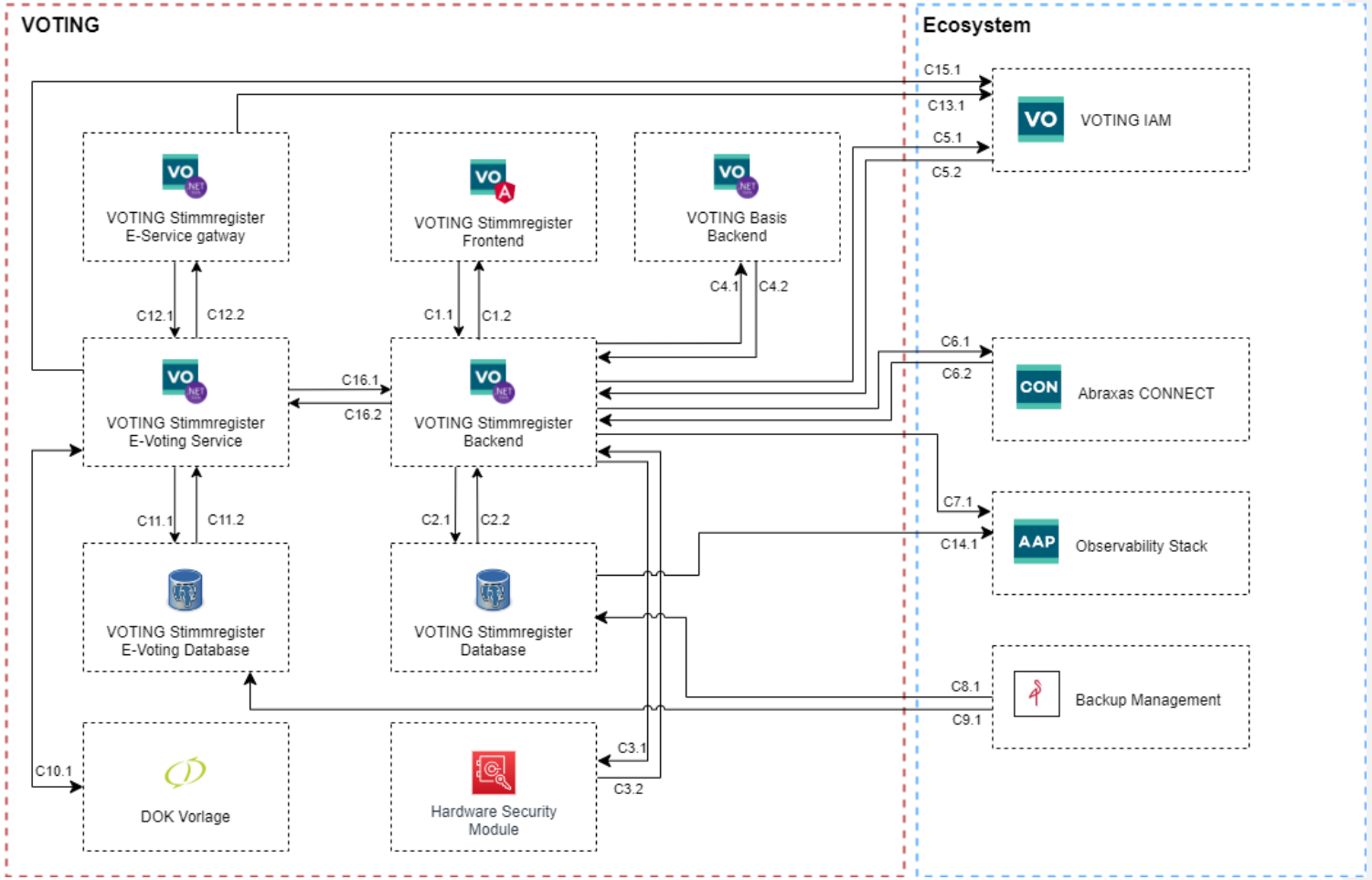
Für die digitale Schweiz. Mit Sicherheit.

Contents

1. Transport Security

In the following section, the transport security, i.e. the connection security, between the various system components is shown.

1.1 Visualization


VOTING
Ecosystem
VOTING Stimmregister E-Service gatway
VOTING Stimmregister Frontend
VOTING Basis Backend
VOTING Stimmregister E-Voting Service
VOTING Stimmregister Backend
VOTING Stimmregister E-Voting Database
VOTING Stimmregister Database
DOK Vorlage
Hardware Security Module
VOTING IAM
Abraxas CONNECT
Observability Stack
Backup Management
C15.1
C13.1
C5.1
C5.2
C12.1
C12.2
C1.1
C1.2
C4.1
C4.2
C16.1
C16.2
C6.1
C6.2
C11.1
C11.2
C2.1
C2.2
C7.1
C14.1
C8.1
C9.1
C10.1
C3.1
C3.2

1.2 System Communication

Data flow	Consumer System	Source system	Encryption	Cluster internal*	Authorization mechanism	Comments
C1.1, C1.2	VOTING Stimmregister Frontend	VOTING Stimmregister Backend	HTTPS	No	OpenId Connect (User Account)	OIDC based code flow with PKCE and client-side refresh flow.
C2.1, C.2.2	VOTING Stimmregister Backend	VOTING Stimmregister Database	-	Yes	Basic credentials	
C3.1, C3.2	VOTING Stimmregister Backend	Hardware Security Module	-	Yes	PIN	The communication with the HSM library is established via PKCS #11. An authentication key is used for mutual authentication purposes.
C4.1, C4.2	VOTING Stimmregister Backend	VOTING Basis Backend	-	Yes	OAuth 2.0 Client Credential (Service User)	
C5.1, C5.2	VOTING Stimmregister Backend	VOTING IAM	HTTPS	No	OAuth 2.0 Client Credential (Service User)	
C6.1, C6.2	CONNECT Business Service	VOTING Stimmregister Backend	HTTPS	No	OAuth 2.0 Client Credential (Service User)	
C7.1, C7.2	VOTING Stimmregister Services	Observability Stack	-	Yes	-	All backend services are connected with the observability stack using the same technical setup for data delivery.
C8.1	Backup Management	VOTING Stimmregister Database	-	Yes	-	
C9.1	Backup Management	VOTING Stimmregister E-Voting Database	-	Yes	-	
C10.1	VOTING Stimmregister E-Voting Service	DOK Vorlage	HTTPS	Yes	Basic credentials	

Commented [DS1]: Ist in einem Dokument "Transport Security" die Beschreibung der Security mit dem Begriff "HTTPS" genau genug?

Möchte es nur zur Diskussion stellen. TLS-Versionen und sogar Cipher-Suiten zu beschreiben machen das Dokument auf jeden Fall wieder fragil bzw. sehr änderungsintensiv… bin mir auch unsicher.

Commented [GA2R1]: Wird als offene Punkt für Public Bug Bounty aufgenommen.

Commented [JG3R1]: Ich lasse es vorerst auf HTTPS für den 8.2.24. Entspricht auch dem Entscheid welchen wir damals mit Darius für Ausmittlung getroffen haben. Können das aber gerne nochmals besprechen und für später aufnehmen. Die restlichen Anpassungen in den Dokumenten habe ich umgesetzt.

Data flow	Consumer System	Source system	Encryption	Cluster internal*	Authorization mechanism	Comments
C11.1, C11.2	VOTING Stimmregister E-Voting Service	VOTING Stimmregister E-Voting Database	-	Yes	Basic credentials	
C12.1, C12.2	VOTING Stimmregister E-Service Gateway	VOTING Stimmregister E-Voting Service	-	Yes	OAuth 2.0 Client Credential (Service User)	
C13.1	VOTING Stimmregister E-Service Gateway	VOTING IAM	HTTPS	No	OAuth 2.0 Client Credential (Service User)	
C14.1	VOTING Stimmregister Databases	Observability Stack	-	Yes	-	All databases are connected with the observability stack using the same technical setup for data delivery.
C15.1	VOTING Stimmregister E-Voting Service	VOTING IAM	HTTPS	No	OAuth 2.0 Client Credential (Service User)	
C16.1, C16.2	VOTING Stimmregister E-Voting Service	VOTING Stimmregister Backend	-	Yes	OAuth 2.0 Client Credential (Service User)	