Connectis

Security Checklist

This document provides a checklist of standard security requirements in place for services, Municipalities and Identity Providers connecting to the Connectis eIDAS Broker. Please note this list is not exhaustive and further verification is highly recommended. Implementation requirements and agreements are not part of this public document. Please contact eidastechnical@connectis.nl in case of questions about the security checklist.

Checklist details

Project	eIDAS
Date	
Name of Checklist Performer	
Name of Service	
Name of Service Provider	
Url of Service	

1.1 Design and Threat Modeling[1]

Feature	Implemented (Yes / No)	Details
Clear separation between the application layers		
No sensitive data in client side code		
All application components are free from known vulnerabilities		

1.2 Authentication[2]

Feature	Implemented (Yes / No)	Details
All resources by default require authentication except for those intended to		

[1] References: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure and https://www.owasp.org/index.php/Top_10_2013-A9-Using_Components_with_Known_Vulnerabilities

[2] References: https://www.owasp.org/index.php/Authentication_Cheat_Sheet and https://www.owasp.org/index.php/Fail_securely and https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management

be public		
All authentication controls fail securely to ensure attackers cannot log in		
All authentication decisions can be logged without storing sensitive session identifiers or passwords		
All authentication credentials for accessing external services are stored in a protected location		

1.3 Session Management[3]

Feature	Implemented (Yes / No)	Details
Session manager resistant against all common session management attacks		
Sessions are invalidated after logout		
Sessions timeout after a specified period of inactivity		
Session id is never disclosed in URLs, error messages or logs		
Sessions ids are random and unique		

1.4 Access Control[4]

Users are assigned a well-defined set of roles and privileges.

Feature	Implemented (Yes / No)	Details
Users are only able to access resources for which they have authorization		

[3] References: https://www.owasp.org/index.php/Session_Management_Cheat_Sheet and https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management

[4] References: https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References and https://www.owasp.org/index.php/Access_Control_Cheat_Sheet and https://www.owasp.org/index.php/Guide_to_Authorization

Sensitive records are protected		
Access controls fail securely		
All access control decisions can be logged		

1.5 HTTP Configuration[5]

Feature	Implemented (Yes / No)	Details
Content type header specifying a safe character set in every HTTP response		
X-Frame-Options header set in every HTTP response		
Access-Control-Allow-Origin header set in every HTTP response		

1.6 Input Handling[6]

All input is validated and handled accordingly.

Feature	Implemented (Yes / No)	Details
Buffer overflow protection[7]		
SQL injection protection [8]		
LDAP injection protection[9]		
XPath injection protection[10]		
OS Command injection protection[11]		

[5] References: https://www.owasp.org/index.php/Content_Security_Policy and https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet and https://www.owasp.org/index.php/CORS_OriginHeaderScrutiny
[6] https://www.owasp.org/index.php/Top_10_2013-A1-Injection
[7] https://www.owasp.org/index.php/Buffer_Overflow
[8] https://www.owasp.org/index.php/SQL_Injection
[9] https://www.owasp.org/index.php/LDAP_injection
[10] https://www.owasp.org/index.php/XPATH_Injection
[11] https://www.owasp.org/index.php/Command_Injection

Remote/Local file inclusion protection[12]		
CSRF protection[13]		
Replay attack protection[14]		
XSS attacks protection[15]		
XML poisoning protection[16]		
HTTP parameter pollution attacks protection[17]		
All input data is validated[18]		
Authenticated data is cleared from client storage after the session is terminated		

1.7 Cryptography[19]

Access to keys is managed in a secure manner.

Feature	Implemented (Yes / No)	Details
Cryptographic algorithms are validated against FIPS 140-2 or an equivalent standard		
Explicit policy for how keys are managed		

[12] https://www.owasp.org/index.php/Top_10_2007-A3
[13] https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF) and https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
[14] https://www.owasp.org/index.php/Testing_for_WS_Replay_(OWASP-WS-007)
[15] https://www.owasp.org/index.php/Top_10_2013-A3-Cross-Site_Scripting_(XSS) and https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
[16] http://www.ws-attacks.org/XML_Injection
[17] https://www.owasp.org/index.php/Testing_for_HTTP_Parameter_pollution_(OTG-INPVAL-004)
[18] https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet
[19] References: https://www.owasp.org/index.php/Guide_to_Cryptography and https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet and https://www.owasp.org/index.php/Top_10_2010-A7

1.8 Error Handling and Logging[20]

All logged information is handled securely and logging sensitive information is disabled unless specifically required.

Feature	Implemented (Yes / No)	Details
No error messages or stack traces containing information that could assist an attacker are logged		
No sensitive data is logged		

1.9 Data Protection[21]

Data should be protected from unauthorized disclosure or modification and should be available to authorized users as required.

Feature	Implemented (Yes / No)	Details
Data stored in client side storage does not contain sensitive information		

1.10 Communication Security[22]

Feature	Implemented (Yes / No)	Details
All connections that involve sensitive information are authenticated		
Only strong algorithms, ciphers and protocols are used		
The communications use protected channels		

[20] https://www.owasp.org/index.php/Error_handling and https://www.owasp.org/index.php/Error_Handling,_Auditing_and_Logging and https://www.owasp.org/index.php/Improper_Error_Handling

[21] References: https://www.owasp.org/index.php/Data_Security and https://www.owasp.org/index.php/User_Privacy_Protection_Cheat_Sheet

[22] References: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet and https://www.owasp.org/index.php/Top_10_2010-A9