



Securing Mobile Apps with the MASVS.

Our Journey to v2.0

Sven Schleier

7th July 2022 @ OWASP New Zealand



OWASP
**NEW
ZEALAND**
owasp.org.nz



QUANTUM
SECURITY



Cyber**CX**

DATACOM



snyk



Auth0

Checkmarx



HCL AppScan

kordia



**LATERAL
SECURITY**



**MICRO
FOCUS**



Pulse Security
www.pulsesecurity.co.nz



RedShield



Flux

SEQA
Information Security



Cobalt



LACEWORK



SecureFlag

Without them, OWASP New Zealand Day couldn't happen



Technical Director @WithSecure in Singapore



Sven Schleier

OWASP Mobile Security Testing Guide
Flagship Project Co-Leader

 [@bsd_daemon](https://twitter.com/bsd_daemon)

1. OWASP Mobile Security Project & Resources
2. Google's ADA and the Data Safety Section
3. OWASP MASVS Refactoring Process



OWASP Mobile Security Project & Resources

OWASP Mobile Security Testing Guide

[Main](#)[How-To](#)[Donation Packages](#)[News](#)[FAQ](#)[Acknowledgements](#)

owasp flagship project

 Stars MSTG

9.1k

 Stars MASVS

1.4k

 Follow

2.8k

MSTG release version v1.4.0

MASVS release version v1.4.2

Our Mission

“Define the industry standard for mobile application security.”

This OWASP flagship project provides a security standard for mobile apps (OWASP MASVS) and a comprehensive testing guide (OWASP MSTG) that covers the processes, techniques, and tools used during a mobile app security test, as well as an exhaustive set of test cases that enables testers to deliver consistent and complete results.



<https://owasp.org/www-project-mobile-security-testing-guide/>




Mobile App Security
Verification Standard

*Established security baseline for
mobile apps*



Mobile Security
Testing Guide

*Cookbook for mobile app
security testing*



Mobile Application Security
Verification Standard

OWASP MASVS v1.0.0 (2020-11-11) (commit: d0c6141)
OWASP MASVS v1.4.0 (commit: 494030a)

Architecture, Design and Threat Modeling Requirements

ID	MSTG-ID	Detailed Verification Requirement	L1	L2	R	Android	iOS	Status
1.1	MSTG-ARCH-1	All app components are identified and known to be needed.	Pass	Pass		Open	Pass	Pass
1.2	MSTG-ARCH-2	Security controls are never enforced only on the client side, but on the respective remote endpoints.	Pass	Pass		N/A	N/A	Pass
1.3	MSTG-ARCH-3	A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	Pass	Pass		N/A	N/A	Pass
1.4	MSTG-ARCH-4	Data considered sensitive in the context of the mobile app is clearly identified.	Pass	Pass		N/A	N/A	N/A
1.5	MSTG-ARCH-5	All app components are defined in terms of the business functions and/or security functions they provide.	Pass	Pass		N/A	N/A	Fail
1.6	MSTG-ARCH-6	A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.	Pass	Pass		N/A	N/A	Fail
1.7	MSTG-ARCH-7	All security controls have a centralized implementation.	Pass	Pass		Open	Pass	Pass

Mobile Security
Testing Checklist

*Checklist for mobile app security testing that links
the MASVS to the MSTG*



[Mobile App Security Verification Standard](#)

Established security baseline for mobile apps

Mobile AppSec Verification Standard

SECURITY REQUIREMENTS

V1: Architecture, Design and Threat Modeling Requirements

V2: Data Storage and Privacy Requirements

V3: Cryptography Requirements

V4: Authentication and Session Management Requirements

V5: Network Communication Requirements
















V6: Platform Interaction Requirements

V7: Code Quality and Build Setting Requirements

V8: Resilience Requirements

- The MASVS is a standard that **defines the security requirements** software architects and developers seeking to develop secure mobile applications
- Offer an **industry standard** that can be tested against in mobile app security reviews.
- Provide specific recommendations as to what level of security is recommended for different use-cases.
- Usage ensures **consistency** of mobile app security when developing / testing an app
- 8 different domains with over 80 requirements
- We offer 13 languages!

Data Storage and Privacy Requirements

ID	MSTG-ID	Detailed Verification Requirement	L1	L2	R	Android	iOS	Status
2.1	MSTG-STORAGE-1	System credential storage facilities need to be used to store sensitive data, such as PII, user credentials or cryptographic keys.				Test Case	Test Case	
2.2	MSTG-STORAGE-2	No sensitive data should be stored outside of the app container or system credential storage facilities.				Test Case	Test Case	
2.3	MSTG-STORAGE-3	No sensitive data is written to application logs.				Test Case	Test Case	
2.4	MSTG-STORAGE-4	No sensitive data is shared with third parties unless it is a necessary part of the architecture.				Test Case	Test Case	
2.5	MSTG-STORAGE-5	The keyboard cache is disabled on text inputs that process sensitive data.				Test Case	Test Case	
2.6	MSTG-STORAGE-6	No sensitive data is exposed via IPC mechanisms.				Test Case	Test Case	
2.7	MSTG-STORAGE-7	No sensitive data, such as passwords or pins, is exposed through the user interface.				Test Case	Test Case	
2.8	MSTG-STORAGE-8	No sensitive data is included in backups generated by the mobile operating system.				Test Case	Test Case	



[Mobile Security
Testing Guide](#)

*Cookbook for mobile app
security testing*

- The MSTG is a *comprehensive manual* for mobile app security testing and reverse engineering.
- It *describes technical processes* for verifying the controls listed in the MASVS.
- Used as reference in case you want to explore a specific test for a requirement in the MASVS

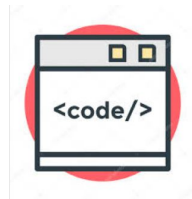


[Mobile Security
Testing Guide](#)

*Cookbook for mobile app
security testing*



Overview



Static Testing



Dynamic Testing

Structure of a test case

Where can I get it?



Github

[MSTG - Github Repo](#)

[MASVS - Github Repo](#)

Gitbook

[MSTG - Gitbook](#)

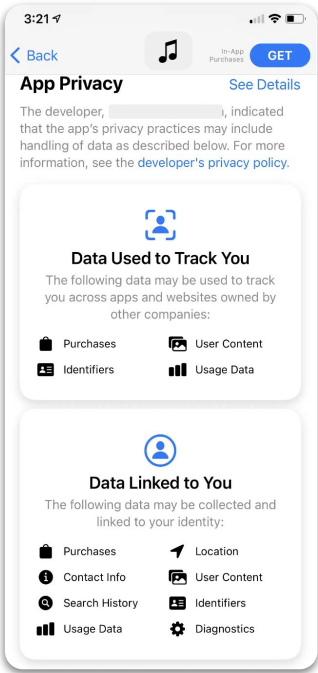
[MASVS - Gitbook](#)

- *Download it*
- *Read it*
- *Use it*
- *Give Feedback and create an issue!*

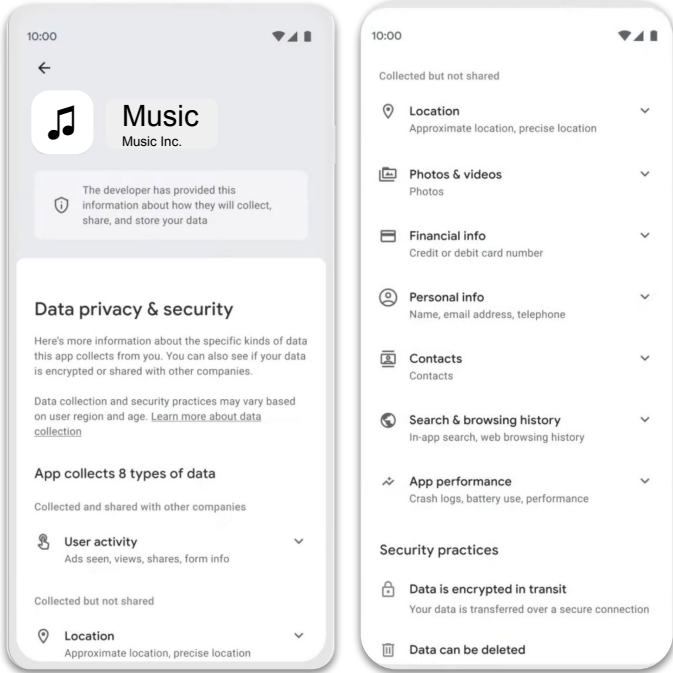


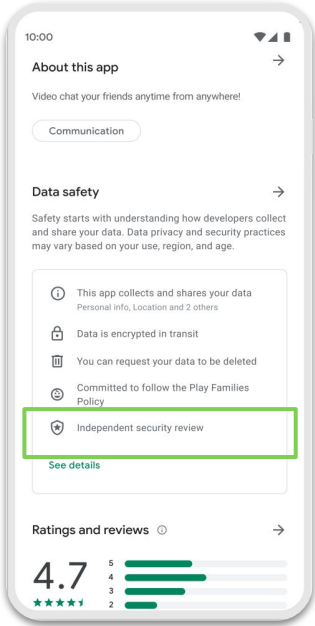
Google's ADA and the Data Safety Section

Apple Privacy Nutrition Labels



Google Data Safety Labels





Thanks to Google's App Defense Alliance (ADA), Developers can showcase **key privacy and security practices**, at a glance.

By [July 20th 2022](#), the Data safety section for all your apps must be approved.



[App Defense Alliance: Mobile Application Security Assessment](#)



OWASP MASVS Refactoring Process

MASVS

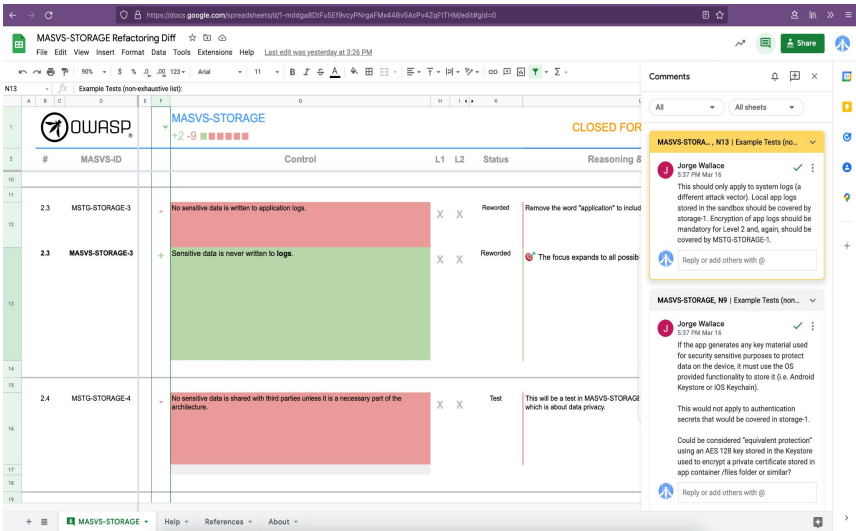
Mobile Application Security Verification Standard



Sven Schleier
Bernhard Mueller

Carlos Holguera
Jeroen Willemsen

- MASVS-NETWORK
- MASVS-CRYPTO
- MASVS-STORAGE
- MASVS-PLATFORM
- MASVS-CODE
- MASVS-AUTH
- MASVS-RESILIENCY
- MASVS-ARCH

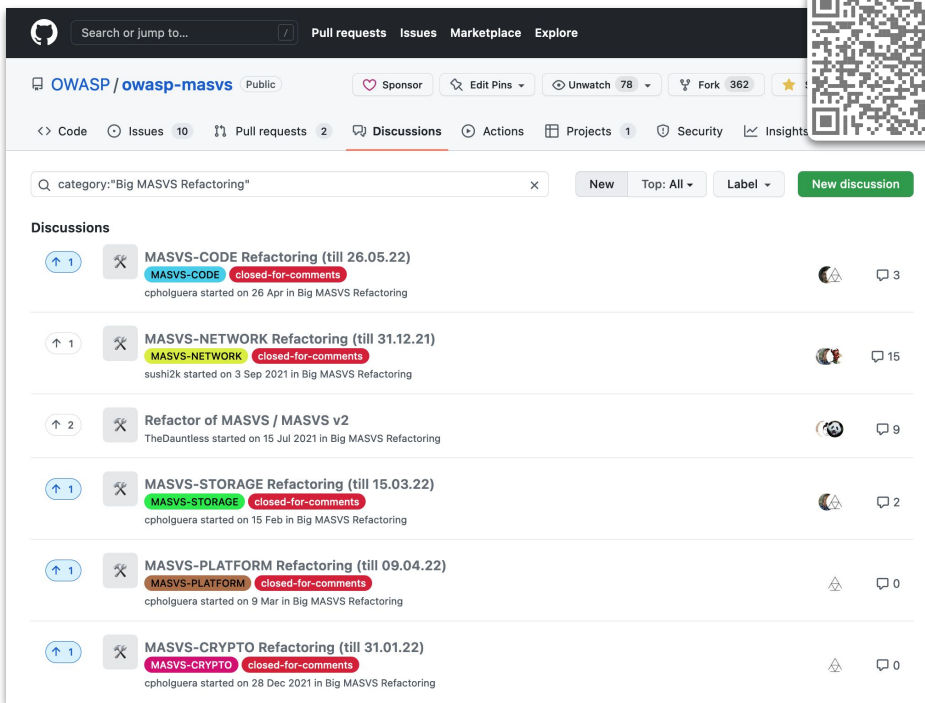


The screenshot shows a Google Docs document titled "MASVS-STORAGE Refactoring Diff". The document is a table with columns for MASVS-ID, Control, L1, L2, Status, and Reasoning. It lists several MASVS-STORAGE controls, including MASVS-STORAGE-3 and MASVS-STORAGE-4. The document is marked as "CLOSED FOR" and includes comments from Jorge Wallace. The table content is as follows:

MASVS-ID	Control	L1	L2	Status	Reasoning	
2.3	MSTG-STORAGE-3	No sensitive data is written to application logs.	X	X	Reworded	Remove the word "application" to include
2.3	MASVS-STORAGE-3	Sensitive data is never written to logs.	X	X	Reworded	The focus expands to all possib
2.4	MSTG-STORAGE-4	No sensitive data is shared with third parties unless it is a necessary part of the architecture.	X	X	Test	This will be a test in MASVS-STORAGE which is about data privacy.

OWASP MASVS Refactoring Process

How to access & Contribute



Search or jump to...

Pull requests Issues Marketplace Explore

OWASP / owasp-masvs Public

Sponsor Edit Pins Unwatch 78 Fork 362

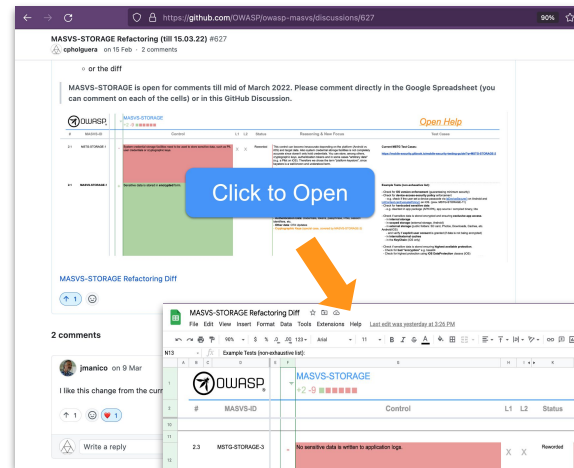
Code Issues 10 Pull requests 2 Discussions Actions Projects 1 Security Insights

category:"Big MASVS Refactoring"

New Top: All Label New discussion

Discussions

- MASVS-CODE Refactoring (till 26.05.22)**
closed-for-comments
cpholguera started on 26 Apr in Big MASVS Refactoring
- MASVS-NETWORK Refactoring (till 31.12.21)**
closed-for-comments
sushizk started on 3 Sep 2021 in Big MASVS Refactoring
- Refactor of MASVS / MASVS v2**
TheDauntless started on 15 Jul 2021 in Big MASVS Refactoring
- MASVS-STORAGE Refactoring (till 15.03.22)**
closed-for-comments
cpholguera started on 15 Feb in Big MASVS Refactoring
- MASVS-PLATFORM Refactoring (till 09.04.22)**
closed-for-comments
cpholguera started on 9 Mar in Big MASVS Refactoring
- MASVS-CRYPTO Refactoring (till 31.01.22)**
closed-for-comments
cpholguera started on 28 Dec 2021 in Big MASVS Refactoring



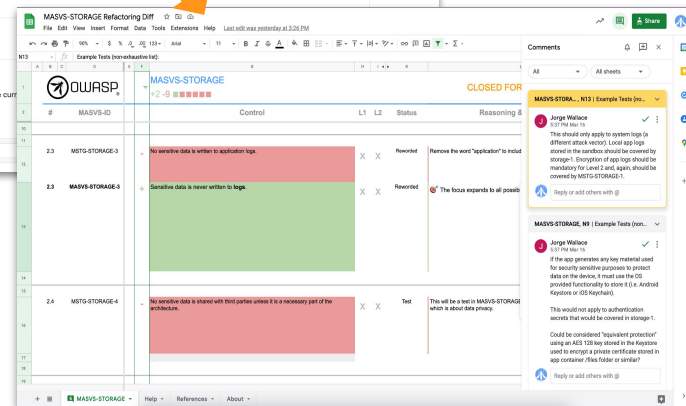
MASVS-STORAGE Refactoring (till 15.03.22) #627

gholguera on 15 Feb · 2 comments

or the diff

MASVS-STORAGE is open for comments till mid of March 2022. Please comment directly in the Google Spreadsheet (you can comment on each of the cells) or in this GitHub Discussion.

Click to Open



MASVS-STORAGE Refactoring Diff

Example Tests (non-vulnerable list)

MASVS-ID	Control	L1	L2	Status	Reasoning
2.3	MSTG-STORAGE-3	No sensitive data is written to application logs	X	Reverted	Remove the word "application" is invalid
2.3	MASVS-STORAGE-3	Sensitive data is never written to logs	X	Reverted	The focus expands to all possible
2.4	MSTG-STORAGE-4	No sensitive data is shared with third parties unless it is a necessary part of the production	X	Test	This will be a test in MASVS-STORAGE which is about data privacy

Comments

MASVS-STORAGE... N13 | Example Tests (non-vulnerable list)

Jorge Wallace 15 Feb 16:16

This should only apply to system logs (a different attack vector). Local app logs stored in the sandbox should be covered by storage. (Exception of app logs should be mandatory for user data and app data should be covered by MSTG-STORAGE-1)

Reply or add others with @

MASVS-STORAGE... N13 | Example Tests (non-vulnerable list)

Jorge Wallace 15 Feb 16:16

If the app generates any key material used for security sensitive purposes to protect data on the device, it must use the OS provided functionality to store it (i.e. Android KeyStore or iOS Keychain).

This would not apply to authentication secrets that would be covered in storage-1. Could be considered "equivalent protection" using an AES 128 key stored in the KeyStore used to encrypt a private certificate stored in app container (this false or not?)

Reply or add others with @

Example: Detecting inconsistencies & overlapping

MSTG-STORAGE-1

System credential storage facilities need to be used to store sensitive data, such as PII, user credentials or cryptographic keys.

1. “System credential storage” vs KeyChain/KeyStore
 - a. What about Android Account Manager?
2. “Sensitive data, such as PII” is not meant to be in the platform KeyStore

MSTG-STORAGE-2

No sensitive data should be stored outside of the app container or system credential storage facilities.

1. Overlaps with 1
2. Sometimes data must live outside

MSTG-STORAGE-13

No sensitive data should be stored locally on the mobile device. Instead, data should be retrieved from a remote endpoint when needed and only be kept in memory.

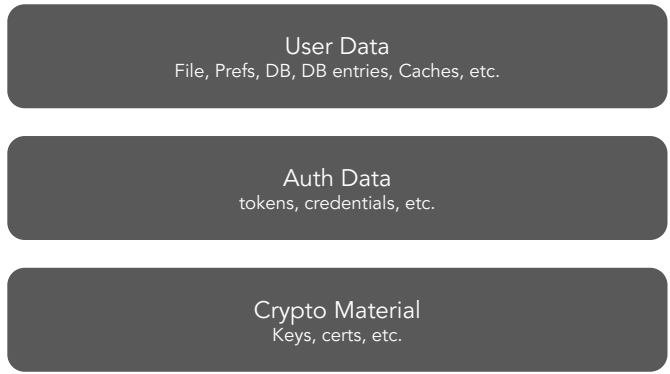
1. Overlaps with the 1 and 2
2. More an architectural decision

Example: Redefining the scope

Architecture



Scope



* "User Data" Source: <https://developer.android.com/guide/topics/data/collect-share>

Example

MSTG-STORAGE-1 (System credential storage)

MSTG-STORAGE-2 (outside of the app container)

MSTG-STORAGE-3 (logs)

MSTG-STORAGE-4 (3rd party data share)

MSTG-STORAGE-5 (keyboard cache)

MSTG-STORAGE-6 (IPC)

MSTG-STORAGE-7 (UI exposure)

MSTG-STORAGE-8 (backups)

MSTG-STORAGE-9 (UI background)

MSTG-STORAGE-10 (memory)

MSTG-STORAGE-11 (device-access-security policy)

MSTG-STORAGE-12 (privacy)

MSTG-STORAGE-13 (no local data)

MSTG-STORAGE-14 (HW-backed encrypted + auth)

MSTG-STORAGE-15 (wipe after failed auth)

MASVS-STORAGE-1

Sensitive data is stored in **encrypted** form.

MASVS-STORAGE-2

Cryptographic keys are stored inside the **platform keystore** or using equivalent protection.

MASVS-STORAGE-3

No sensitive data is written to application **logs**.

MASVS-STORAGE-4

No sensitive data lives in **memory** longer than necessary, and is cleared after use.

MASVS-STORAGE-5

The app follows data **privacy** best practices when processing sensitive user data.

Example: Moving controls to other categories

- MSTG-STORAGE-1 (System credential storage)
- MSTG-STORAGE-2 (outside of the app container)
- MSTG-STORAGE-3 (logs)
- MSTG-STORAGE-4 (3rd party data share)
- MSTG-STORAGE-5 (keyboard cache)
- MSTG-STORAGE-6 (IPC)
- MSTG-STORAGE-7 (UI exposure)
- MSTG-STORAGE-8 (backups)
- MSTG-STORAGE-9 (UI background)
- MSTG-STORAGE-10 (memory)
- MSTG-STORAGE-11 (device-access-security policy)
- MSTG-STORAGE-12 (privacy)
- MSTG-STORAGE-13 (no local data)
- MSTG-STORAGE-14 (HW-backed encrypted + auth)
- MSTG-STORAGE-15 (wipe after failed auth)

MASVS-PLATFORM

MASVS-CRYPTO

MASVS-STORAGE-1

Sensitive data is stored in **encrypted** form.

MASVS-STORAGE-2

Cryptographic keys are stored inside the **platform keystore** or using equivalent protection.

MASVS-STORAGE-3

No sensitive data is written to application **logs**.

MASVS-STORAGE-4

No sensitive data lives in **memory** longer than necessary, and is cleared after use.

MASVS-STORAGE-5

The app follows data **privacy** best practices when processing sensitive user data.

Example: Moving controls to other categories

MSTG-STORAGE-1 (System credential storage)

MSTG-STORAGE-2 (outside of the app container)

MSTG-STORAGE-3 (logs)

MSTG-STORAGE-4 (3rd party data share)

MSTG-STORAGE-5 (keyboard cache)

MSTG-STORAGE-6 (IPC)

MSTG-STORAGE-7 (UI exposure)

MSTG-STORAGE-8 (backups)

MSTG-STORAGE-9 (UI background)

MSTG-STORAGE-10 (memory)

MSTG-STORAGE-11 (device-access-security policy)

MSTG-STORAGE-12 (privacy)

MSTG-STORAGE-13 (no local data)

MSTG-STORAGE-14 (HW-backed encrypted + auth)

MSTG-STORAGE-15 (wipe after failed auth)

MASVS-PLATFORM

MASVS-CRYPTO

MASVS-STORAGE-1

Sensitive data is stored in **encrypted** form.

MASVS-STORAGE-2

Cryptographic keys are stored inside the **platform keystore** or using equivalent protection.

MASVS-STORAGE-3

No sensitive data is written to application **logs**.

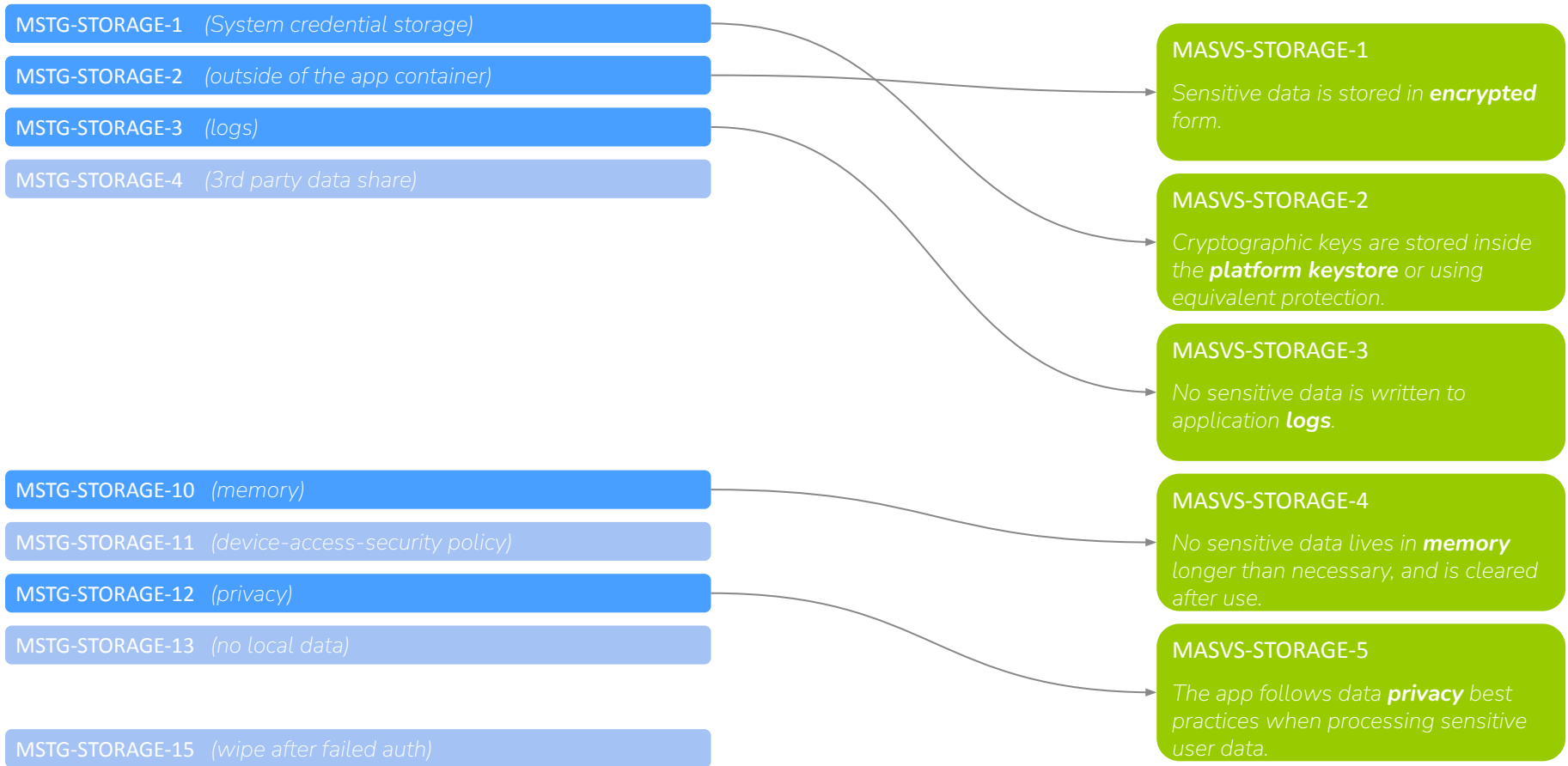
MASVS-STORAGE-4

No sensitive data lives in **memory** longer than necessary, and is cleared after use.

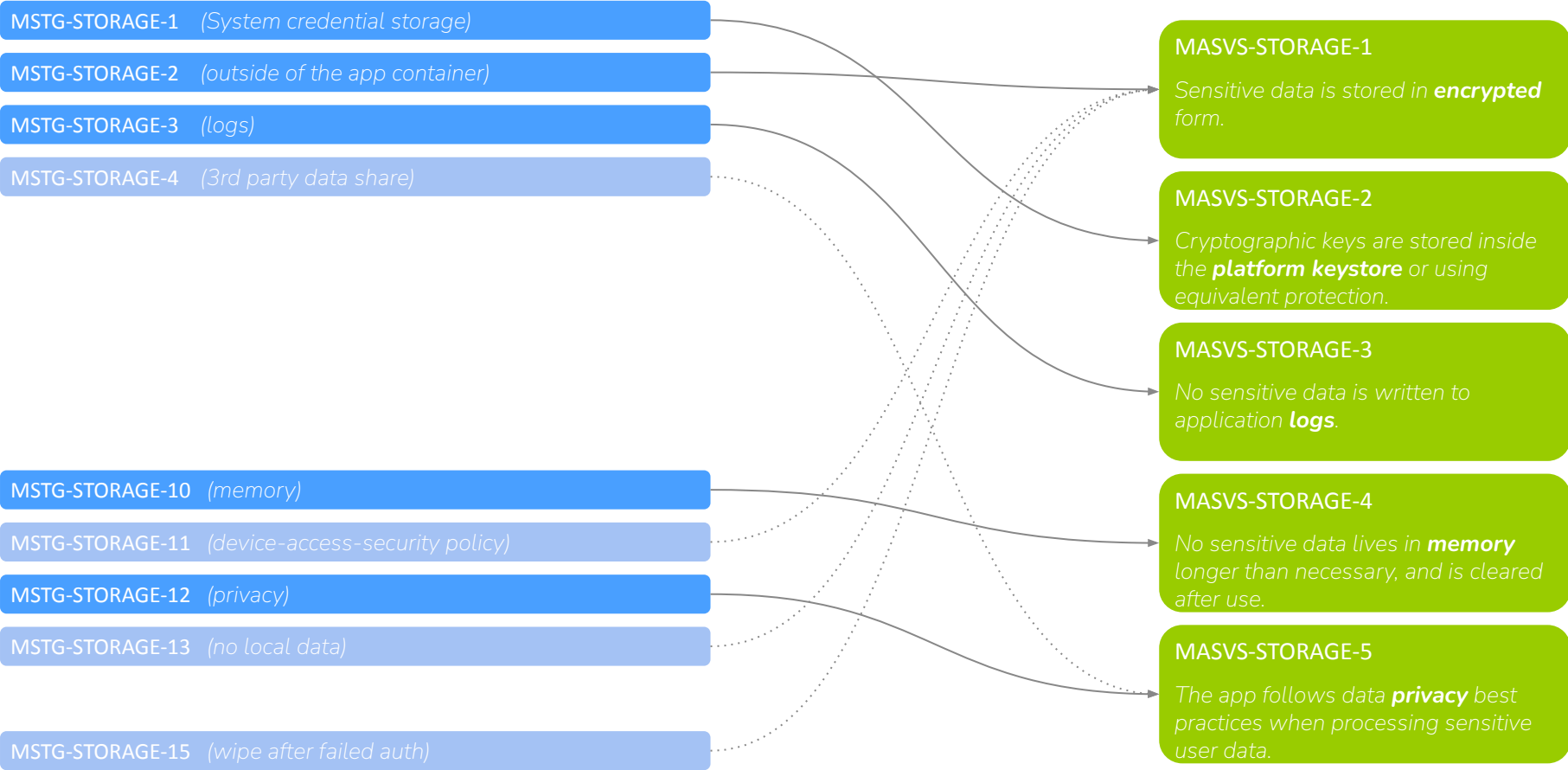
MASVS-STORAGE-5

The app follows data **privacy** best practices when processing sensitive user data.

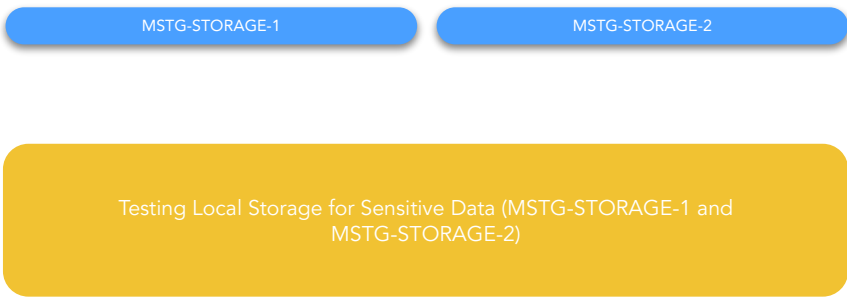
Example: Establishing the new controls



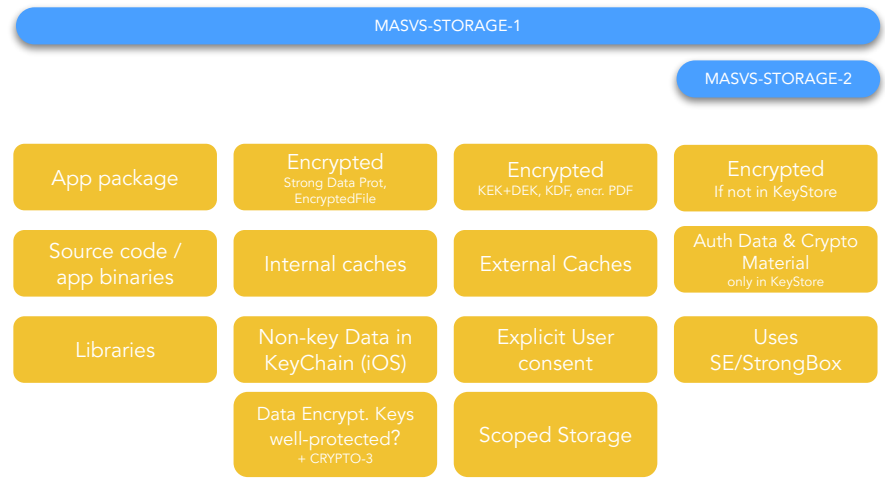
Example: Identifying tests



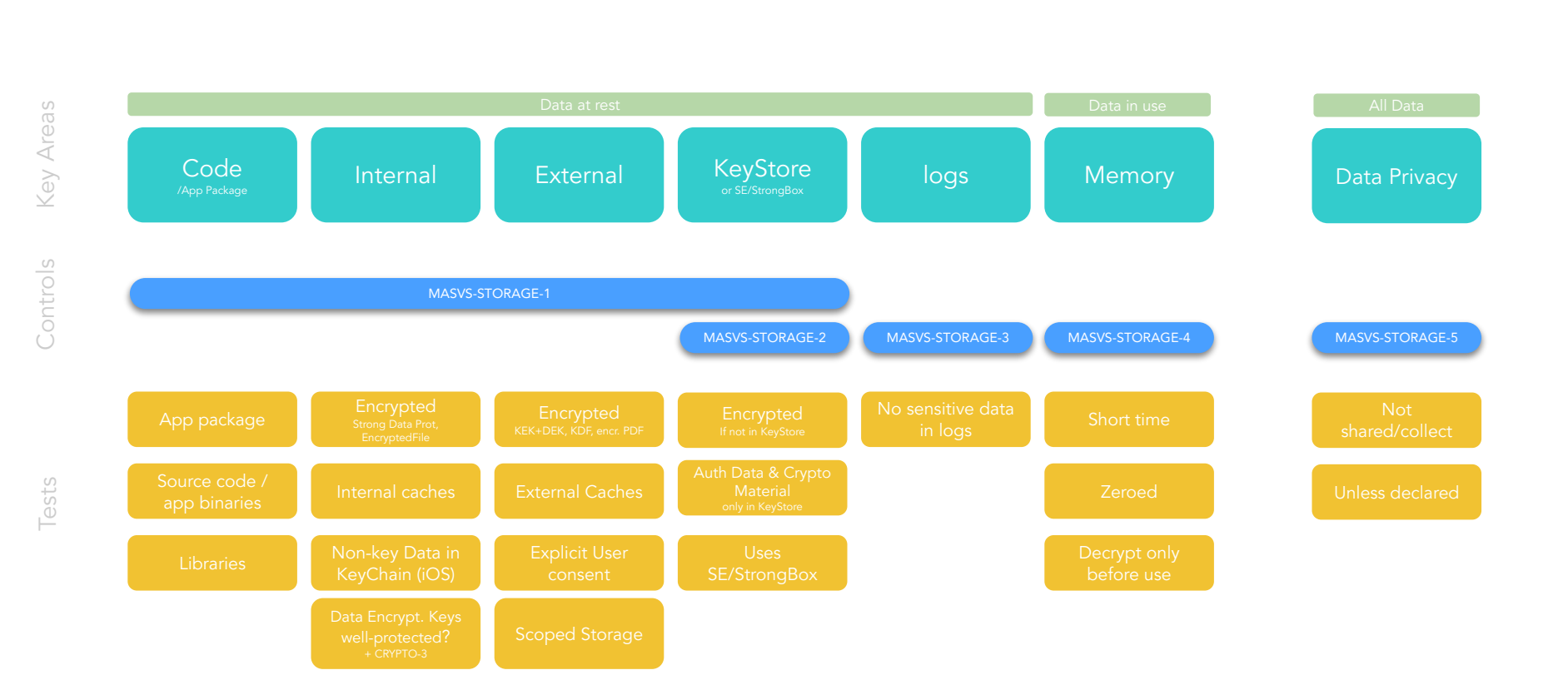
MSTG V1



MSTG V2
with “Atomic Tests”



Putting all together





OWASP MASVS Compliance-as-Code

Human
+
excel/PDF/Word



Automation
+
yaml/json/xml



MASVS

L1

L2

Mobile Application Security Verification Standard

R

Privacy

Automation-friendly

IoT

Health

Sven Schiesser
Bernhard Mueller

OWASP

MASVS
provided

Community
created

- Read and interpret manually
- Hard to prove control and test coverage
- Compare providers manually
- Hard to maintain

- Machine-readable
- Easy to prove control and test coverage
- Compare providers with benchmarking
- Fully traceable

Standard and fully tailored testing

MASVS + proprietary + cross-standards



Get in Touch



 [@OWASP_MSTG](https://twitter.com/OWASP_MSTG)

 [owasp-masvs](https://github.com/owasp-masvs)

 [owasp-mstg](https://github.com/owasp-mstg)

 [project-mobile_omtg](https://project-mobile-omtg.org)

 projects/MSTG



 [@grepharder](https://twitter.com/grepharder)

 Carlos.Holguera@owasp.org

 [carlos-holguera](https://www.linkedin.com/in/carlos-holguera)

 [cpholguera](https://github.com/cpholguera)

 [Carlos](https://github.com/Carlos)



 [@bsd_daemon](https://twitter.com/bsd_daemon)

 Sven.Schleier@owasp.org

 [sven-schleier](https://www.linkedin.com/in/sven-schleier)

 [sushi2k](https://github.com/sushi2k)

 [Sven](https://github.com/Sven)

Fix
typos

Improve our
Android / iOS
Crackme apps

Review PRs

Enhance / write
new Test Cases

Try out new
hacking tools



Design our Swag

Help us automate &
GitHub Actions

Answer
Discussions

Give feedback
to the MASVS
Refactoring

Contribute & connect with us!

<https://github.com/OWASP/owasp-mstg#connect-with-us>

...



Thank
you!



Mobile Security Research Engineer
NowSecure

Carlos Holguera

OWASP Mobile Security
Testing Guide Flagship
Project Co-Leader

 @grepharder



Technical Director
WithSecure (Singapore)

Sven Schleier

OWASP Mobile Security
Testing Guide Flagship
Project Co-Leader

 @bsd_daemon