Defence Assurance Platform
Authenticating Government Media

Australian Government
Defence

The Australian Defence Force (ADF) is the military organization responsible for the defense and security of Australia and its national interests. The ADF operates as a unified and integrated force comprising the Royal Australian Navy (RAN), the Australian Army, and the Royal Australian Air Force (RAAF). Its primary mission is to protect Australia from external threats, contribute to regional and global security, and assist in natural disasters or humanitarian crises.

Challenge

The Australian Defence Force (ADF) produces a range of public media products each week, including press releases, images of operations, and videos showcasing its activities. However, once this data is available online, it's susceptible to alterations and falsifications.

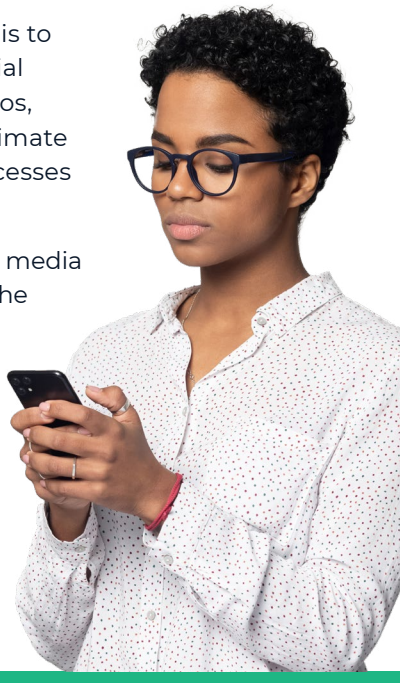
As a result, the ADF must ensure that documents and media released online are authenticated, accurate and genuine. This functionality is critical given the ADF shares content across multiple online-facing platforms. Without adequate oversight, AI-generated deep-fakes and other falsified press can undermine credibility and destabilize civilian life.

Goal

The goal of the **Defence Assurance Platform** is to allow content recipients to authenticate official public media releases, including images, videos, and press releases, verifying that each is legitimate ADF-released media. There are two main processes supported to facilitate this:

- **Registration Process:** The publically released media is stored by the platform and secured using the blockchain, ensuring it's tamper-proof.
- **Verification Process:** Arbitrary media is compared against officially released media previously registered.

Ensuring the authenticity of released media supports transparency and accountability while protecting the ADF's reputation as a trusted defense organization.



Technical Details

The SIMBA Chain solution allows authenticated actors to upload images, video, and text to the **Defence Assurance Platform**, where metadata (including digital fingerprints) are extracted and committed to the blockchain. Through this mechanism, the system provides verifiable proof that data has been registered to an immutable ledger—here's how it works:

Media Fingerprints

Cryptographic hashes are a common way of creating digital fingerprints for the following reasons:

- Hashes are content-based and can be used to match files exactly.
- Hashes give "Yes" or "No" answers if they are identical, bit for bit.

However, videos and images use codecs (e.g., jpg, png, mp4, mov) and contain metadata. This data changes even when an image or video is exactly the same. As such, syntactic hashes were used to provide a degree of match for media content.

Syntactic Fingerprints

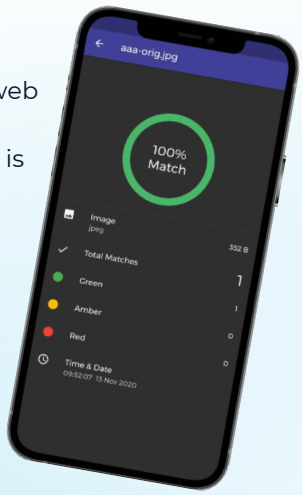
Syntactic hashes create efficient, comparable digital fingerprints that support:

- Comparison between different media types (e.g., images are 256bit and videos are 256KB).
- Searching through thousands of records in a fraction of a second.
- Providing a degree of match output (0-100)—0 is not a match, and 100 means it matches exactly.
- Determining the degree to which the media has been changed.
- Utilizing open source algorithms (PDQ and TMK + PDQF) initially created by Facebook.

Platform Components

The Defence Assurance Platform comprises three functional layers:

1. **Backend API:** The backend API manages data and media comparisons (e.g., images and Fotoweb connect directly to the API). During this process, a syntactic hash is generated for each media item, which enables comparison to the presented media. Finally, a hash of each syntactic hash is stored on the blockchain, authenticating each one while eliminating hacks and other attacks.
2. **Backend Web App:** Used to upload original media like images, PDFs, videos, and press releases.
3. **Frontend Mobile App (iOS and Android):** Built with Google Flutter, the mobile app matches media, supporting the easy-to-understand scoring mechanism (0-100). This metric provides users with a level of confidence when authenticating the data they possess. Uploaded content is also categorized as green, amber, and red—with green indicating higher matching content, while amber and red indicate content with lower matching content.



About SIMBA

Incubated at the University of Notre Dame in 2017, SIMBA Chain (short for Simple Blockchain Applications) provides a scalable enterprise platform that simplifies blockchain development. With fewer barriers to entry, companies can build secure, scalable, enterprise-grade solutions that integrate seamlessly with existing data systems. SIMBA implementations generate value for major government organizations, enterprises, and blockchain companies as a production-grade platform that enables public, private, or hybrid deployments.