Jabra GN

WHITE PAPER

JABRA DECT WIRELESS

The time to Engage is now

The most powerful, professional Digital Enhanced Cordless Telecommunications(DECT) wireless headsets on the market are now Common Criteria, EAL2

Taking security with communication devices to the next level: 256-bit, beyond Step C, DSAA2 encryption

Multiple Cyber Threats nullified.
Cut their connection.

SECURING BUSINESS-SENSITIVE CONVERSATIONS

Cybercrime rose nearly 13% in the 2020/2021 financial year, and in the Government and private sector business environment where phone calls are ever more sensitive, securing valuable conversations is critical.

When reviewing DECT devices for ASD certification in 2021, ASD found four disturbing vulnerabilities with the “headset” piece of equipment for Federal Government environments, which increase the risk of cybersecurity threats.

The common method of over the air pairing is a huge vulnerability allowing four key areas of vulnerability such as Masquerade, Weak Crypto, Eavesdrop, and Tamper.

- A **masquerade** attack happens when a fake identity imitates the access identification to gain access to a device. Attackers can easily reach all of the organisation’s important data once they gain access. The list of cybercrime opportunities includes stealing confidential data, modifying or deleting data, changing the network configuration and routing information. The authorization process must be fully protected to avoid this.

- When a cryptographic key (**weak crypto**) is compromised, it becomes more susceptible to attacks. Keys need to be larger to keep up with the increasing computational powers, and encryption keys must not be revealed. More than one root key may be needed to control the damage if a single key is uncovered.

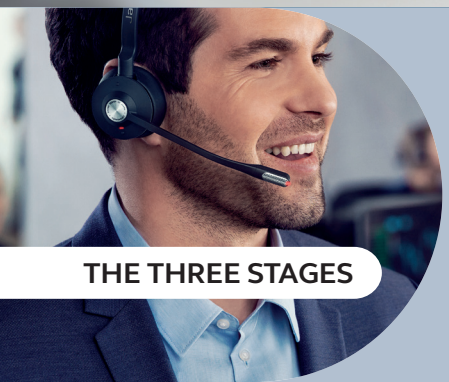
- To prevent an **eavesdropping** attack, network communications need to be secured to stop attackers from intercepting the data being transmitted between two devices. Such vulnerabilities are common in public Wi-Fi networks that are not encrypted. When sensitive data is sent across an open network, it gives hackers leeway to take advantage of a vulnerability and intercept data.

- Cybersecurity threats can also take root in the physical hardware. Addressing hardware-based security risks requires anti-tamper protection and **tamper-resistant hardware**. A device with tamper-resistant security module (TRSM) usually offers the following: tamper-resistance, a hardened casing on the device which makes attacks challenging; tamper-evident, which allows users to see that an intrusion attempt was made as indicated by a broken seal; and tamper-responsive, which identifies the attack attempt and remove the data.

These four threats were present in wired as well as wireless equipment in Federal Government offices and environments. These uncertainties form the basis of the Common Criteria on our Engage 65 and 75 devices for our EAL2 Certification.

Taking communication security to the next level, Jabra’s Engage 65 and 75 Series meets these challenges head-on with it's secure professional DECT wireless headsets. Every call counts, but for some businesses and institutions, the ability to make secure calls can make or break a company, safeguard the future of others, and even save lives. Whether you’re a government, the military, a financial institution, or simply a business where valuable calls are made, you need to be part of a proactive security culture.

The time to Engage is now.



THE THREE STAGES

PAIRING

AUTHENTICATION

ENCRYPTION

The solution: Jabra Engage headsets

Patented pairing, 256-bit AES encryption. 128-bit authentication, ASD certified excellence.
With Jabra Engage, there is increased security of the wireless connection between the wireless headset and its base unit, and rock-solid security is provided in three steps, improving the protection of calls to a category-leading level.

PAIRING

To ensure that the base unit and headset work in tandem, they need to be physically bonded through Jabra's patented 'physical assisted pairing' method. This technique can only be completed when the headset is first docked in the base unit. Next, the secure link-key is created when the base unit and headset are successfully paired. The mutual authentication of the base unit and headsets increases the security of the devices and ensures that any malicious device trying to masquerade as a legitimate headset or base unit are detected immediately.

AUTHENTICATION

Once a call starts, a secure authentication between the Engage headset and its base unit is set up via encryption. The headset and base unit will only work together when a link is established using a secret key-link formed when both devices are paired. The authentication link is also protected by 256-bit encryption. Users will only be able to use the headset when properly paired with the base unit. As calls are encrypted, anyone trying to listen in will not be able to divulge the content of the communication between headset and base unit. This applies to anywhere within the premises or within the proximity of the premises where the wireless communication spreads.

ENCRYPTION

By using 256-bit AES encryption, the highly secured pairing and authentication gives a line of defence that is higher than DECT Security Level C. To prevent malicious users from attempting and succeeding in reversing the process of encryption on Jabra Engage, the encryption link is refreshed every single minute. This makes decryption much harder and reduces security threats.

SECURITY FEATURES COMPARED:

SECURITY FEATURES	JABRA ENGAGE 75/65	EPOS SD W 5000 SERIES	POLY SAVI 8200 SERIES
Pairing	Physical assisted, patented pairing	Physical assisted, patented pairing	
Authentication	128 bit DSAA2 (AES)	128 bit DSAA2 (AES)	64 bit DSAA
Encryption	256 bit AES	128 bit AES	64 bit DSC
DECT security level	beyond C	B	A
ASD Certification	Yes	No	No

To serve and protect

DECT IN DETAIL.

DECT security has evolved over time from the original security definition to new enhanced definitions called step A, B, and C; each step offering an increase in security. Each new security level includes all features from a previous level. Jabra Engage achieves all requirements, and goes beyond DECT Level C.

Jabra Engage utilizes AES 256-bit keys, enhanced custom versions of DSAA2 and DSC2 for the very strongest level of encryption in a professional headset.

Enterprise Grade

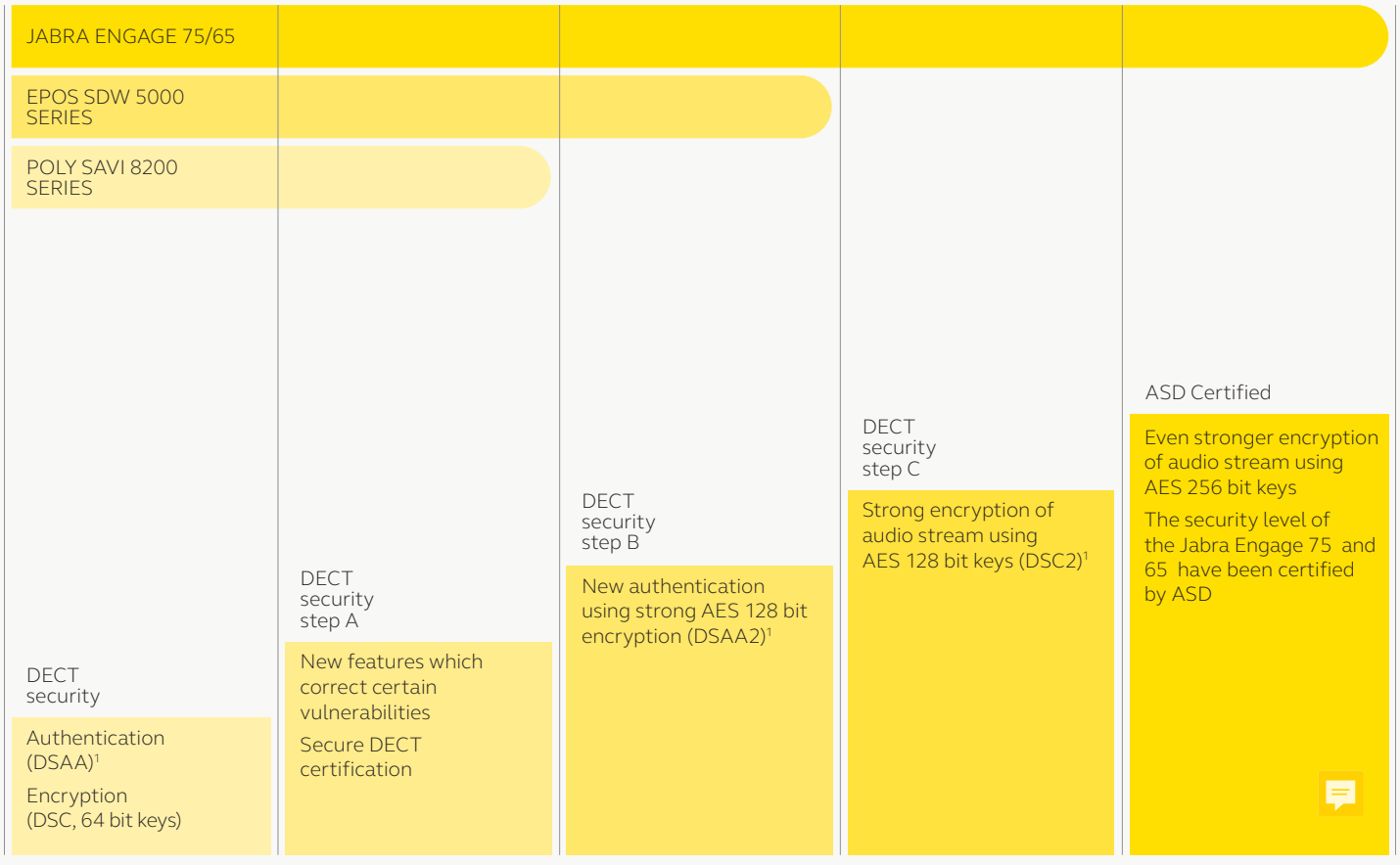
The Engage 65 and 75 use 256-bit enhanced custom versions of DSAA2 and DSC2 instead of the 128-bit security. The devices have been certified using the EAL2 testing program and are the only secure headset listed on the Common Criteria.

Commonly referred to as Common Criteria or CC, The Common Criteria for Information Technology Security Evaluation is an international standard for computer security certification. It allows products to be evaluated by proficient and licensed laboratories to ensure they fulfil certain security properties. Computer security products that are Common Criteria certified have gone through the rigorous and standardized process of specification, implementation and evaluation.

Having met an agreed-upon security standard for government deployments, Engage 65 and 75 give users the added assurance of the products' level of security.

The DSAA2 protocol is enhanced to use 256-bit challenges and responses for authentication and for generation of a 256-bit DCK. The protocol is otherwise identical to the standard DSAA2.

Encryption excellence



[1] DSAA and DSC are the authentication and encryption algorithms defined in the DECT security standard ETSI EN 300 175-7 applicable for DECT security and DECT security step A. DSAA2 and DSC2 are the equivalent updated security algorithms for the next steps of DECT security, steps B and C.

More about Jabra Engage Series wireless headsets

FINAL SUMMARY

- The **security level** of Common Criteria EAL2 for the Jabra Engage 65 and 75 DECT wireless headsets has been certified and tested by the Australian Signals Directorate.
- **Provides superior wireless connectivity** to a range of up to 150 meters/490 feet, enabling up to 3x more users in the same office space – with no loss in connection quality.
- Advanced **noise canceling microphones** and enhanced speakers deliver crystal-clear calls even in noisy offices.
- **All day battery life** and a busylight that acts as a do-not-disturb sign for colleagues.

ENGAGE 65

ENGAGE 75

Different working environments, office layouts and interiors present an almost infinite variety of challenges when planning the effective deployment of multiple wireless headsets in a limited space. As a world-leading supplier of wireless headset solutions, Jabra has many years of experience helping customers deploy effective wireless solutions on their premises.

WHAT IS ASD?

Part of the national security infrastructure in Australia, the Australian Signals Directorate (ASD) is Australia's foreign signals intelligence, cyber security and offensive cyber operations agency.

With the main purpose of defending Australia from global threats, ASD provides foreign signals intelligence (SIGINT), cyber security and offensive cyber operations, in support of the Australian Government and Australian Defence Force (ADF).

* Only the Engage 75 and Engage 65 are ASD certified

Find out more

If you have any questions about security with Jabra products, please contact your Jabra representative or visit **Jabra.com**

WHO WE ARE

We engineer technology that makes life look and sound better. Our world-leading headsets, intelligent video technology and advanced earbuds make sure life and work stay wonderfully in tune.

Jabra Security Whitepaper A4 110822_v1