Go Sign Desktop Client
Support and release policy

T2 CG – 26 June 2025

Support vs Certification

- **Support is provided by the official Vendor (Ascertia), which is the only one able to provide patches and new versions.**

- **Current supported version by Ascertia for the TARGET Services: 6.9.0.20 and 8.3.6 (all fix packs)**

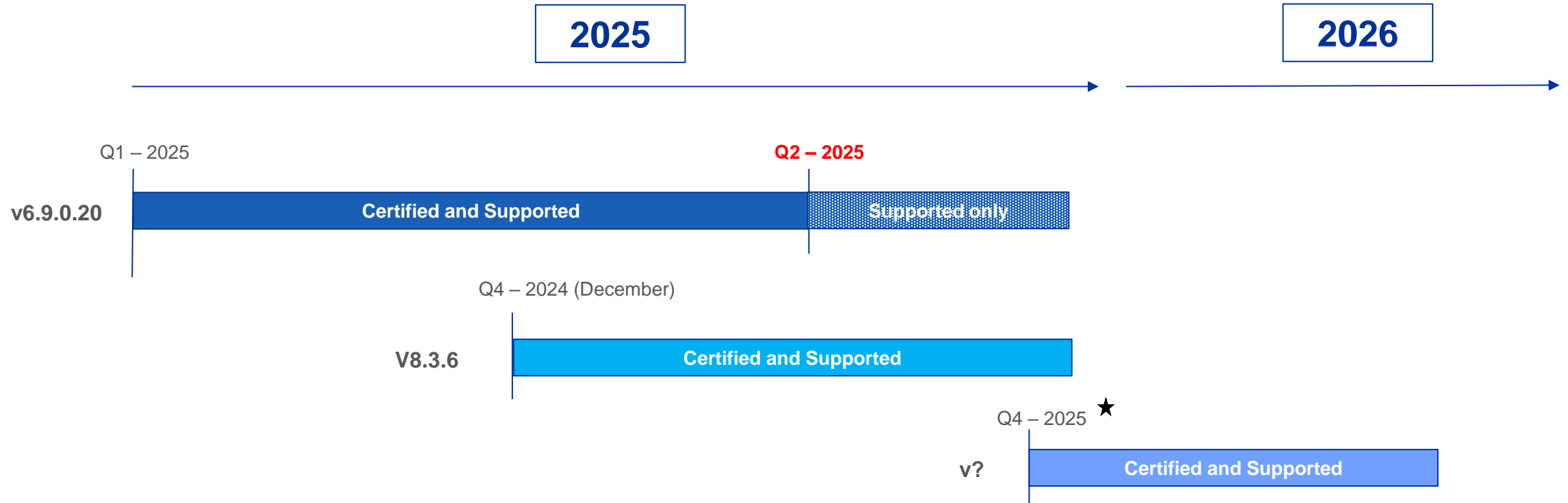- **Within the supported versions, patches are always provided on top of the latest available fix pack**

Certification Advantages

- **Certification is done by the 4CB:**

- **Up to two versions in parallel can be certified by the 4CB (the most up-to-date)**

- **Currently certified versions are <u>6.9.0.20 and 8.3.6</u>**

- **Certified versions include security fixes and cumulative patches (and may already address the customer problem).**

- **Certified versions are subject to full 4CB regression test in addition to tests performed by the vendor. Only certified releases can be downloaded from the ESMIG Portal**

- **When a ticket is opened on a certified version, 4CB can provide more assistance in reproducing issue, providing additional evidences to speed up Ascertia analysis.**

General release policy

- One new version per year will be released

- This new version will either be an updated fix pack within the same major release (as it happened in 2023) or belong to a new major version (as it happed in 2024)

- Fix packs to solve urgent security vulnerabilities can be released at any time according to the criticality (scoring) of the vulnerability

Original Roadmap 2024-2025

2025

2026

Q1 – 2025

Q2 – 2025

v6.9.0.20 | Certified and Supported | Supported only

Q4 – 2024 (December)

V8.3.6 | Certified and Supported

Q4 – 2025 ★

v? | Certified and Supported

★ *Clarifications on-going with Ascertia to establish if a new release is going to happen in 4Q 2025, due to an ongoing update to be delivered in June of the 8.3.6*

5

Current Status:

- **A Bug fixing release on top of the version 8.3.6 is currently under 4CB internal retesting to address some recently discovered vulnerabilities. The latest estimation is to have the fix rolled out by the end of June.**

- **Version 6.0.9.20 is not affected by this vulnerability:**
  - Support and certification period will be extended till end of Q3 to avoid that customers are obliged to install the version 8.3.6 before the fix is released to keep the certification status.