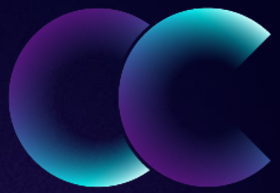
Confidential Compute Working Group (WG) Kickoff



CORECOLLECTIVE

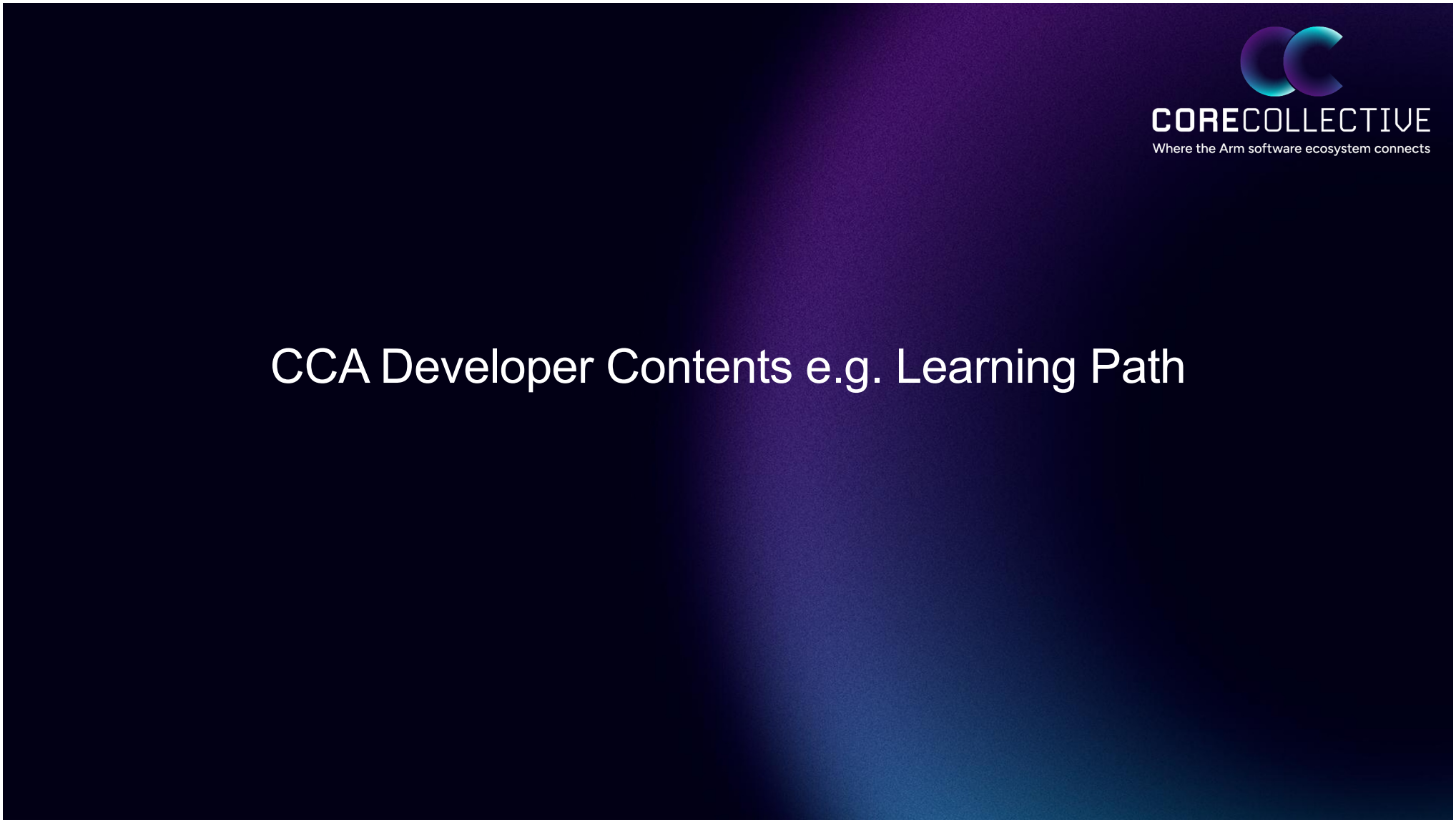
Where the Arm software ecosystem connects

22nd June 2026

Confidential Compute WG Agenda 8th June 2026

CORECOLLECTIVE
Where the Arm software ecosystem connects

- CoreCollective News
- Arm CCA RME Developer Content Intro
- Linaro CCA QEMU Update & Roadmap
- Round the table – CCA Pain Points/Needs


CORECOLLECTIVE
Where the Arm software ecosystem connects
CCA Developer Contents e.g. Learning Path

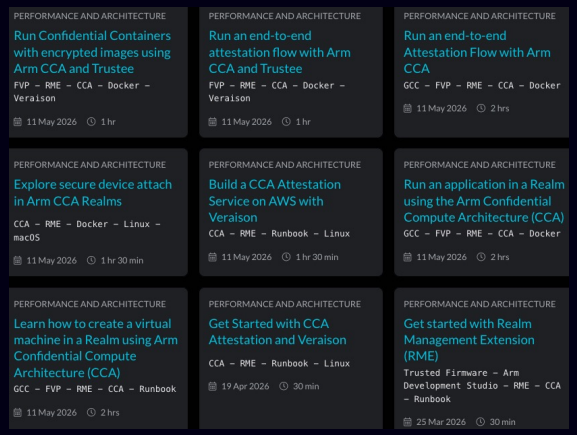
CCA/RME developer enablement content

Support for developers and partners

CORECOLLECTIVE
Where the Arm software ecosystem connects

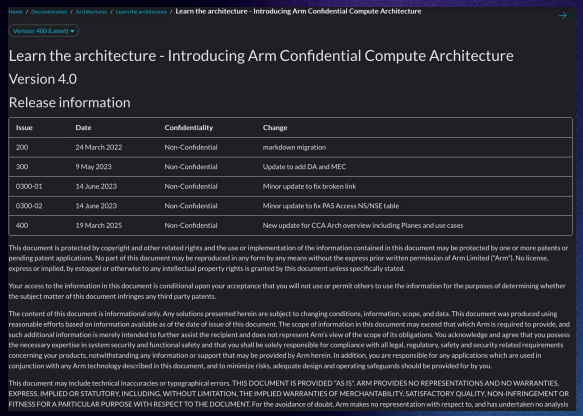
Learning Paths

- https://learn.arm.com/tag/cca
- Demonstrate validated Arm CCA workflows through practical developer content



Documentation

- https://developer.arm.com/documentation/den0125
- Provide end-to-end reference guidance on Arm CCA architecture, attestation and verification


Learn the architecture - Introducing Arm Confidential Compute Architecture
Version 4.0
Release information

Issue	Date	Confidentiality	Change
200	24 March 2022	Non-Confidential	markdown migration
300	9 May 2023	Non-Confidential	Update to add DA and MEC
0300-01	14 June 2023	Non-Confidential	Minor update to fix broken link
0300-02	14 June 2023	Non-Confidential	Minor update to fix PAS Access NS/NSE table
400	19 March 2025	Non-Confidential	New update for CCA Arch overview including Planes and use cases

This document is protected by copyright and other related rights and the use or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm Limited ("Arm"). No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

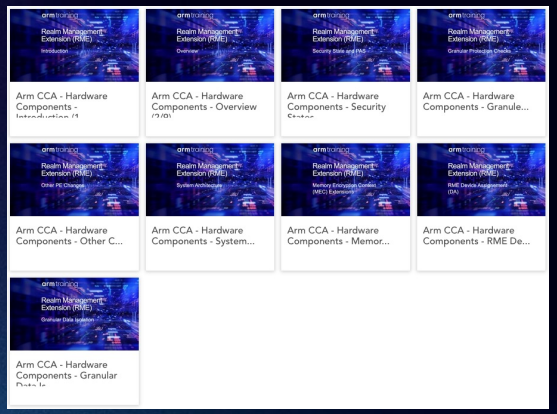
Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether the subject matter of this document infringes any third party patents.

The content of this document is informational only. Any solutions presented herein are subject to changing conditions, information, scope, and data. This document was produced using reasonable efforts based on information available as of the date of issue of this document. The scope of information in this document may exceed that which Arm is required to provide, and such additional information is merely intended to further assist the recipient and does not represent Arm's view of the scope of its obligations. You acknowledge and agree that you possess the necessary expertise in system security and functional safety and that you shall be solely responsible for compliance with all legal, regulatory, safety and security related requirements concerning your products, notwithstanding any information or support that may be provided by Arm herein. In addition, you are responsible for any applications which are used in conjunction with any Arm technology described in this document, and to minimize risks, adequate design and operating safeguards should be provided for by you.

This document may include technical inaccuracies or typographical errors. THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis

Training videos

- https://arm.fuseuniversal.com/topics/164363#
- Provide video-based training that complements the documentation



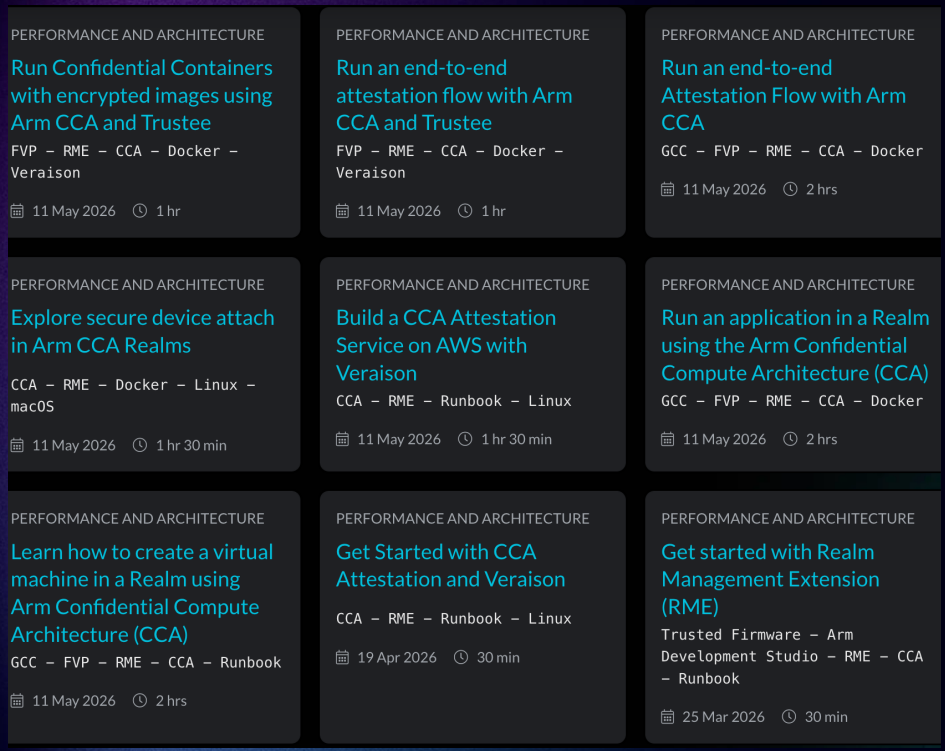
CCA/RME learning paths

Demonstrating validated CCA workflows

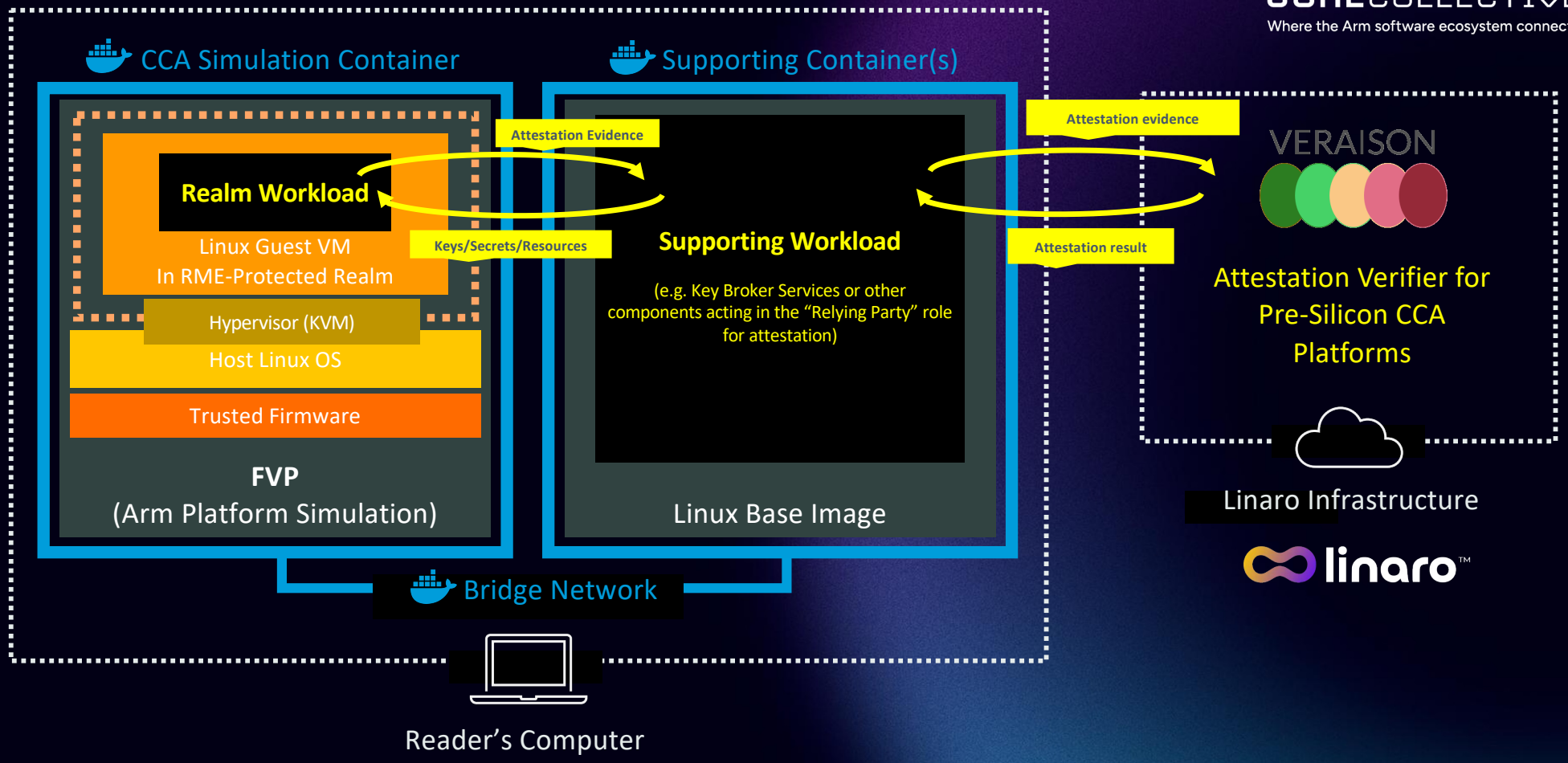
CORECOLLECTIVE
Where the Arm software ecosystem connects

Considerations

- Stack readiness: is there a stable, demonstrable end-to-end workflow?
- Upstream alignment (RMM1.1 → RMM2.0): minimise rework from building on non-upstream branches
- CE software dependencies e.g. Device Attach, P0 Lite, vTPM stack maturity
- Engineering readiness: some areas require additional implementation work first (e.g. Boot Sync attestation)

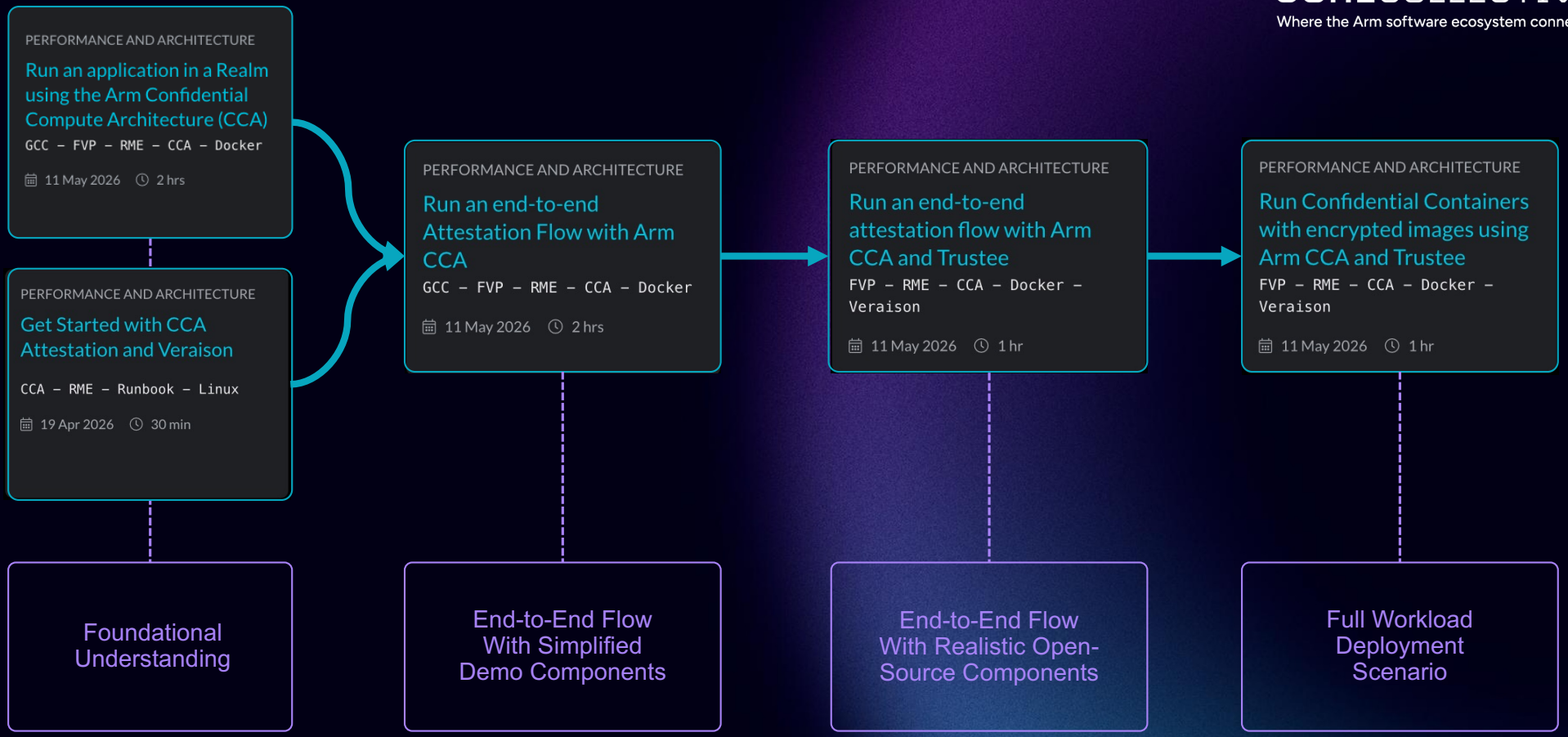


Common Architecture for Attestation Flows



A Progressive Learning Journey

CORECOLLECTIVE
Where the Arm software ecosystem connects

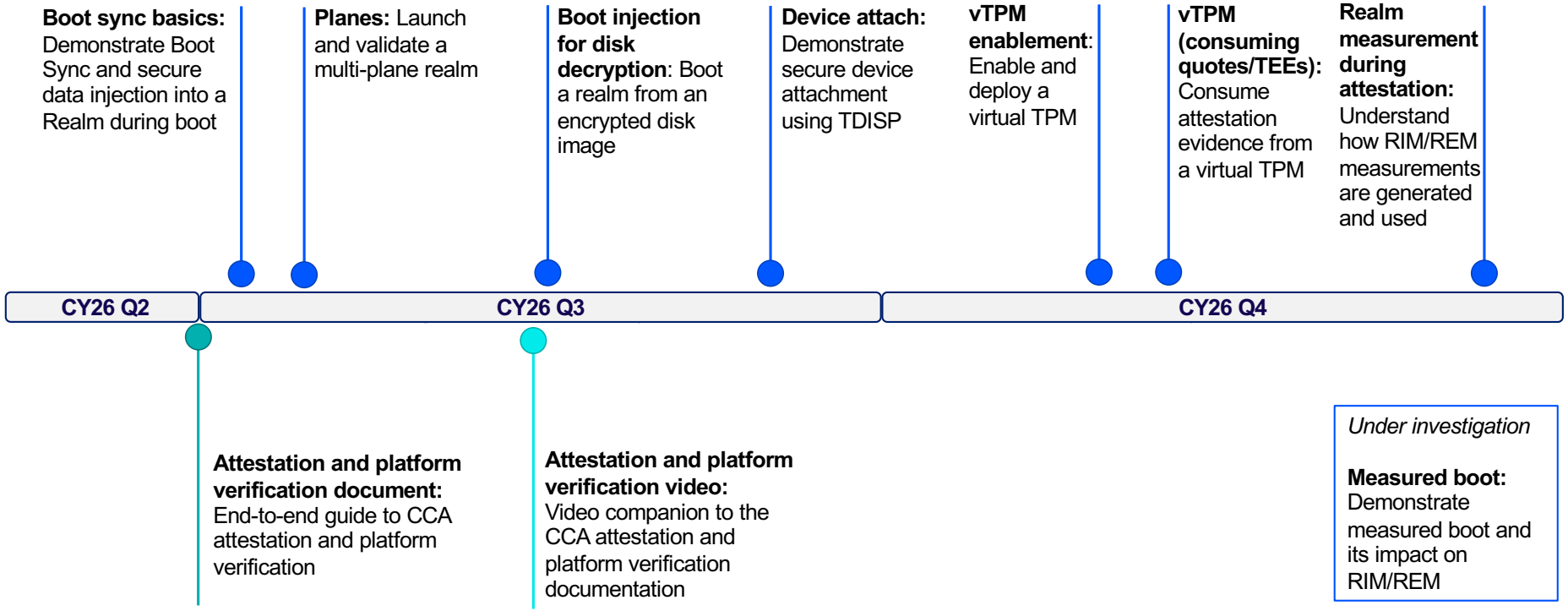


CCA developer enablement roadmap

Learning path
Architecture document
Training video

CORECOLLECTIVE
Where the Arm software ecosystem connects

Provisional timings not committed



Any other business?

CORECOLLECTIVE
Where the Arm software ecosystem connects

- Agenda for next meeting
  - Partners to present Pain points/needs on CCA

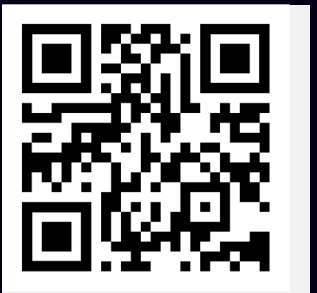

CORECOLLECTIVE
Where the Arm software ecosystem connects
Appendix

Joining the Confidential Compute Working Group

CORECOLLECTIVE
Where the Arm software ecosystem connects

- Join CoreCollective
  - Company: sign and submit Membership Agreement https://corecollective.dev/join/

- After your company has signed the Membership Agreement, please email confidential-compute+subscribe@corecollective.dev from your company email domain
  - Or ”Ask to Join” group from https://groups.google.com/u/0/a/corecollective.dev/g/confidential-compute



CoreCollective.dev

Note: Subscriptions are restricted to company email domains of current members

CoreCollective Terminology

CORECOLLECTIVE
Where the Arm software ecosystem connects

- **Working Group (WG):** A Working Group (WG) is a free-to-join, technology-focused forum for member companies. Its purpose is to target, evangelise, and advance Arm technology within domain-specific verticals (such as Automotive, AI, or Edge Compute) in the Open Source community. Working Groups are typically either standards-based (with no engineering involved) or Initiative-based.
- **WG Initiative:** A WG Initiative is a long-term engineering development effort contained within and guided by a Working Group. Each WG Initiative is funded by Sponsorship from one or more member companies and is executed by an Open Source Solution Provider (OSSP). A WG Initiative may comprise multiple workstreams, but its higher-level focus will reflect a sustained level of effort in Open Source development.
- **Open Source Solution Provider (OSSP):** An Open Source Solution Provider (OSSP) is a specialised engineering firm that bridges commercial requirements and the Open Source ecosystem. OSSPs provide expert development, integration, and long-term maintenance of software stacks (such as the Linux kernel or AI frameworks). They focus on "upstream" contributions to ensure hardware enablement and long-term architectural sustainability for WG Initiatives.
- **Workstream:** a component of work within a WG Initiative. Example: The Virtualisation WG Initiative may include multiple workstreams, such as QEMU, VirtIO, and even a workstream to fund a maintainer for an open-source project.

CoreCollective Terminology continued



- **WG Chair:** Each Working Group is led by a WG Chair, an influential technical expert. The WG Chair is responsible for leading members toward a solution-focused WG Initiative that addresses ecosystem gaps of interest to the broader community. The WG Chair is supported by a CoreCollective Community Manager to guide them efficiently through CoreCollective processes, leading to the deployment of member-desired Initiatives.
- **Community Manager:** For each Working Group, a Community Manager will be assigned to facilitate all WG administrative tasks as defined in the Working Group Life Cycle of the Charter. They will support the WG Chair in driving Initiatives, scheduling/funding support, reporting, and OSSP vendor selection.
- **Technical Advisory Committee (TAC):** The Technical Advisory Committee (TAC) oversees the Working Group. It approves the addition, removal and advancement of Working Groups through the WG Life Cycle.
- **TAC Chair:** The Technical Advisory Committee (TAC) Chair is the individual ultimately responsible for all CoreCollective Collaborative efforts. This person also evangelises CoreCollective membership and is key to determining when to initiate new WGs.