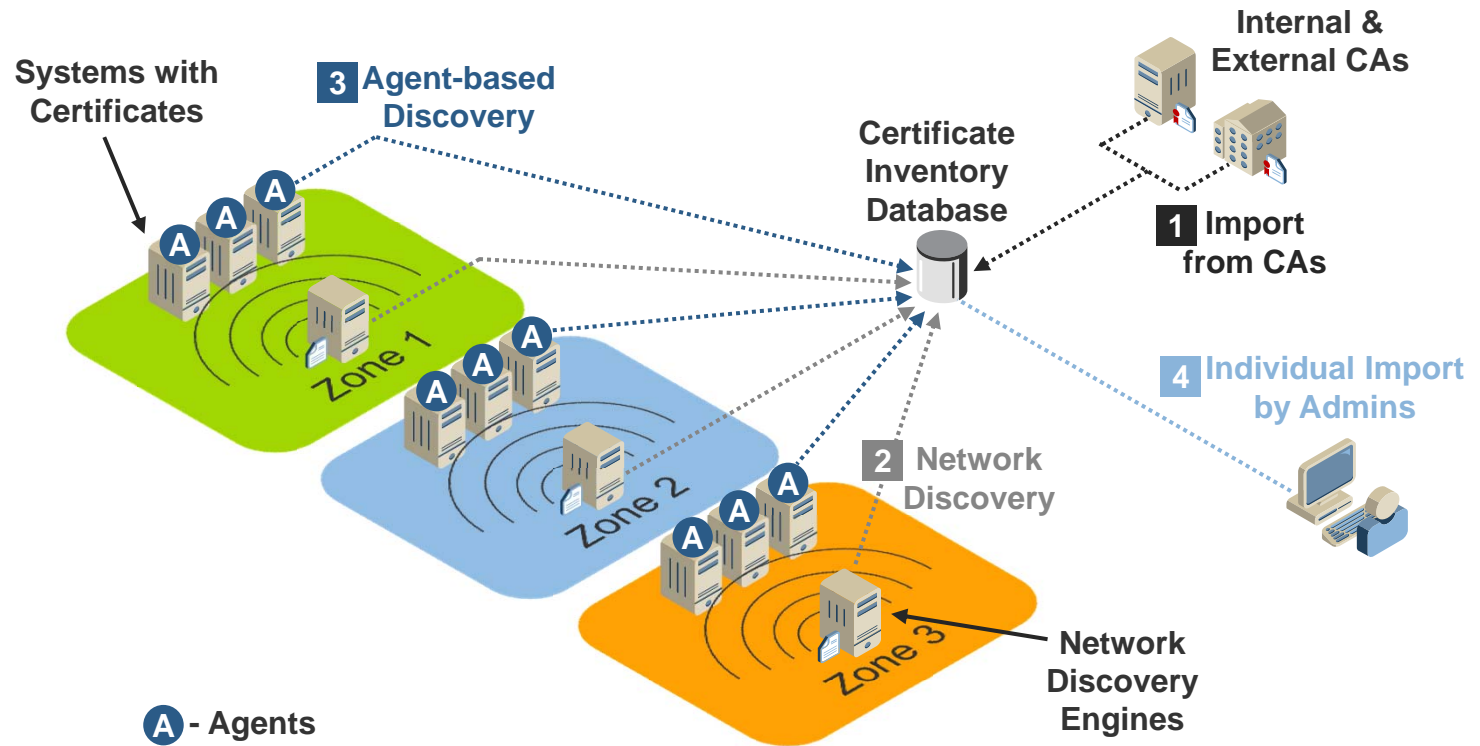




Establishing a Comprehensive Inventory





Analyze Inventory and Evaluate Compliance

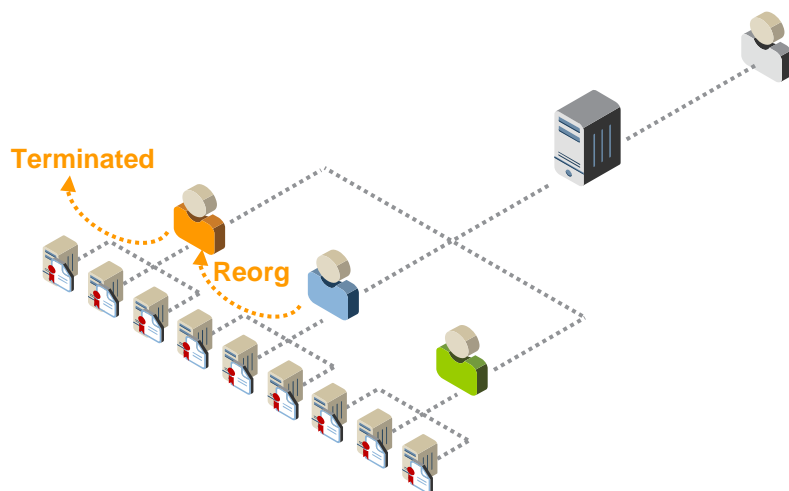


- Certificate authorities/self-signed certificates
- Key lengths
- Signing hash algorithms (e.g. MD5 or SHA1)
- Validity periods
- Expiration dates
- Locations
- Keystore types
- Owners
- Business applications
- Applicable policies and regulations
- Current management processes



Managing Ownership Information

- It is critical to have up-to-date ownership information
 - Notifications for expirations
 - Notifications in case of compromise
 - Invalid notification is worse than no notification at all
- Best to have owners directly manage the updating of information
- Provide central oversight and support





Summary

Preparing for and Responding to CA Compromise

1. Establish an accurate inventory of certificates
 - Identify Owners
2. Ensure only trusted CAs are in use
3. Review CA security
4. Establish backup CA(s)
5. Inventory trust anchors (root certs)
6. Create strategy for rapid certificate replacement (to minimize business interruptions due to CA compromise)
7. Establish method of tracking replacement of certificates



Discussion

Unpublished Work of Venafi, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Venafi, Inc. Access to this work is restricted to Venafi employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Venafi, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

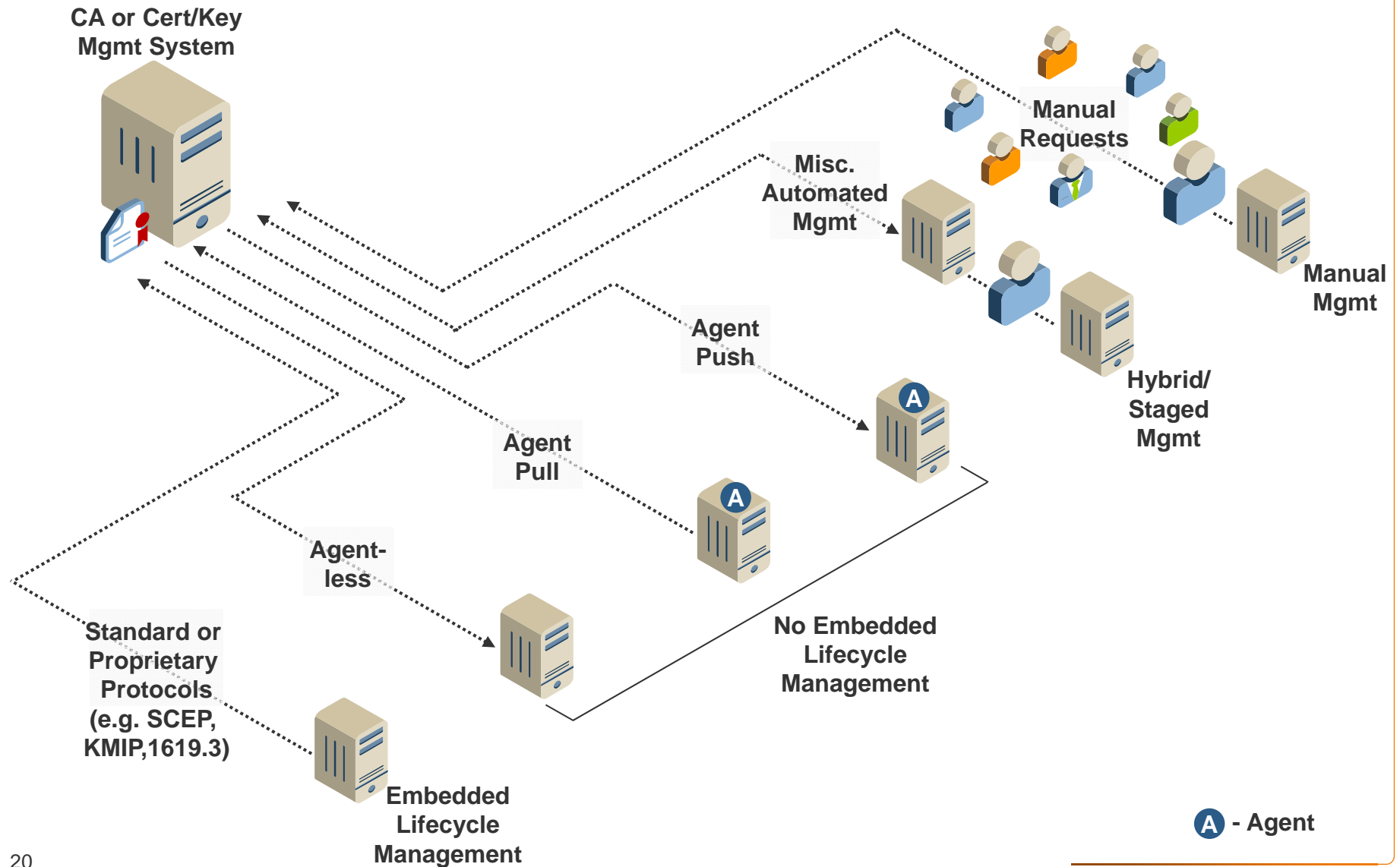
General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Venafi, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Venafi, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Venafi marks referenced in this presentation are trademarks or registered trademarks of Venafi, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.





Encryption Management and Distribution Models



Another Risk: Private Key Security

