HydrantID Response Bulletin

Regarding CA/B Forum Guidance on the Deprecation of Internal Server Names and Reserved IP Addresses

The Certification Authority Browser Forum (CA/Browser Forum) is a voluntary gathering of leading certification authorities (CAs) and vendors of internet browser software and other applications. Members of the CA/Browser Forum have worked closely together in defining the guidelines and means of implementation for best practices as a way of providing a heightened security for internet transactions and creating a more intuitive method of displaying secure sites to internet users.

- **CA/B Forum Internal Host Name Changes:** requires all Certification Authorities (CAs) to stop issuing trusted SSL to internal host names. It's the right thing to do given the potential security risks related to cross-trust and name collision vulnerabilities but has significant operational, security and cost impact on the market. CA/B Forum Guidance and https://cabforum.org/wp-content/uploads/Guidance-Deprecated-Internal-Names.pdf

- **Impact:** Organizations utilizing trusted SSL certificates to secure internal host names may no longer do so. This creates the need to seek other security certificate solutions or change their network architecture and how they manage internal hosts. Both options can be expensive or complex depending on the particular situation.

  There is a big impact on Outlook and Microsoft Exchange implementations when secured by publically trusted SSL certificates (rather than an internal private CA certificate) as without the trusted SSL certificate, Outlook will stop the user with security-warning messages on the Outlook clients. Obviously a not a best practice and bad situation for numerous security and operational reasons.

- **Who is impacted:** Any organization utilizing publicly-trusted SSL certificates to secure their internal hosts. Typically, small to medium sized enterprises, as larger enterprises have the resources to run their own, albeit expensive, private internal CA service.

- **Alternatives[1]:** Some alternatives to consider for impacted organizations:
  - **Change your Network Architecture:** Switch their affected internal IP addresses and any Non-FQDN (i.e. https://mail) to be included under their publically-routable IP name space and then continue to buy publically trusted SSL certificates.

    - *Pros:* Can avoid operating an internal private CA and related complexity and costs.

    - *Cons:* Have to change network architecture and can be operationally challenging to make switch.

- **Run a Private Certificate Authority:** Organizations running their own private internal Certificate Authorities are not impacted, as they have their own trust model and don't rely on the public trust models provided trusted Authorities.

    - *Pros:* Best security and technical solution as organization has complete control of trust model and does not have to change policy or operations related to network architecture. Also, may extend internal CA services to many other security use cases within the organization.

    - *Cons:* Takes significant recourses, expertise and costs to operate within "best practices" as a mission critical security system. Also responsible for Certificate Practices Statement (CPS) and Certificate Policies (CP) for the internal CA. Need to distribute dedicated private root chain to clients and systems through normal patch management process.

- ***Find a Public CA providing "Non-public" Certificates :*** Acquire "non-publically trusted" certificates issued by a Public CA a customer shared issuing CA. *Not considered a viable option from a security perspective as solution does not provide a unique trust anchor and certificate chain.*

    - Pros: No need to change network architecture.

    - Cons: Trust anchor and certificate chain is not unique and is shared by all organizations utilizing the service. Although risks are reduced, the solution does not eliminate cross-trust and name collision vulnerabilities without other network counter measures being deployed. Must also distribute Public CAs "Non-trusted" root certificate chain to all services secured by the "non-publically trusted certificate. Certificate based pricing makes it difficult to plan. Potential for CA to issue identical certificates to multiple organizations, possibly causing name collisions and create potential for mistakes.

- **Utilize HydrantID's Dedicated Issuing Certificate Authority Solution:** HydrantID has an elegant solution that provides organizations the ability to easily secure all of their internal host names with a Dedicated Issuing Certificate Authority (Dedicated ICA). HydrantID's Dedicated ICA provides organizations with benefits they would receive from operating their own private internal certificate authority without the complexity and costs.

- Pros:
  - ***Private Trust Anchor:*** The Dedicated ICA service provides a unique branded issuing CA for each customer. This allows the certificate chain to be unique to each organization and eliminates cross-trust and name collision vulnerabilities.
  - ***Operational simplicity*** - No need to change network architecture; No need to run complex internal Certificate authority operations as service is provided on demand from the cloud by HydrantID
  - ***Security best practices –*** Dedicated ICA provides a unique intermediate root certificate for every customer so their systems can rely on a private unique trust anchor. The Dedicated ICA service is operated to industry best practices
  - ***Control and Flexibility*** - Customer can create their own unique certificate polices and templates and issues certificates on demand- just like a private CA.
  - ***One service for both internal and external host security***- Combine HydrantID's Dedicated ICA service with HydrantID's Subscription SSL service and organizations can secure all internal and external hosts utilizing the same cloud-based SaaS service
  - ***Simple, low cost fixed subscription fee –*** One low cost, fixed subscription fee for all internal and external host certificate needs.

- Cons: Need to distribute dedicated chain to clients and systems through normal patch management process.

- **What are other Certificate Authorities doing?:** Some have chosen to not respond or are recommending their customers change their network architecture. A few are providing non-public certificates from a "customer shared" PKI infrastructure, which does not provide a unique trust anchor for each organization.

[1] Application signed certificates are not considered a viable alternative due to the lack of organizational control with respect to security policy, visibility and operational control.