# Lessons learned, security implications and good practices for branded SubCAs

Publicly-trusted Certification Authority owners (PT-CAs) are foundational to the secure functioning of the Internet. They are entrusted by the general, global public and major browser vendors to provide the essential Public Key Infrastructure (PKI) needed to establish trust, secure communications, and facilitate safe online transactions. To maintain their trustworthiness, publicly-trusted CAs must invest significant resources in the security of their operations and the adherence to the latest standards, and they are subject to rigorous independent audits and supervision.

PT-CAs, as businesses, have a legitimate interest in creating a network of trusted resellers to distribute their products and expand their market presence. Since they act as "trust anchors", they often receive requests from interested parties who would like to include the provision of publicly trusted certificates in their offerings, sometimes under their own name; these are called "white-labeled" or "branded" subCAs.

Many members in the PT-CA, reseller, and subscriber community find branded subCAs valuable to help build reputation without having to invest in a fully dedicated CA infrastructure, and most reseller customers handle the privilege of having their own brand within a SubCA responsibly. Unfortunately, there are cases where poor security practices or abuse, intentional or otherwise, may crop up.

This white paper analyzes the security risks related to branded subCA resellers and suggests good practices based on the experience gathered through our survey and lessons learned from analyzing recent cases in the industry. Our findings should be useful to policymakers (CA/B Forum, Root Store Owners), to PT-CAs who are ultimately responsible for the trustworthiness of their services, and to any other interested party.

# Survey

A survey was conducted by SSL.com in the second half of 2023 to gather insight from the community that would be useful for this report. Our survey included questions that covered the following aspects:

1. Popularity of the branded subCA model
2. Extent of rebranding: branded CRL/OCSP responders, user portals, custom product names
3. Selection/vetting process of branded subCA customers
4. Use of their own user portal
5. Audit and inspection of these portals
6. Lessons learned based on experience with branded subCA customers
7. Technical challenges with generating, controlling, or revoking branded subCAs

The survey was addressed to 9 PT-CAs which, based on analysis of CCADB data, seem to have the most experience with the branded subCA model.

# Survey results

We received responses from 5 out of the 9 PT-CAs, and we followed up for clarifications. Responses were analyzed to identify commonalities and differences in the branded subCA model and relevant practices, as applied by the CA industry.

Highlights of the survey results:

1. Several synonymous terms are being used in the industry for this or similar subCA models: **branded**, **white-labeled**, **dedicated**, **vanity**.
2. 4 out of the 5 participating CAs confirmed that branded subCAs are part of their offerings. The product is targeted to selected customers, such as hosting providers and large resellers. It is also applicable in cases of large accounts that need certificates for their own use; for example, one CA reported applying the model to academic and research institutions.
3. Branding typically includes issuing subCA certificates that have the name of the customer/reseller in the subjectDN field. Extended branding may also include branded CRL/OCSP responder URLs and branded micro-portals for smaller customers/resellers that do not have their own RA portals.
4. The SubCA selection process is mostly based on business/commercial criteria, such as type of activity, forecasted number of certificates, and intended use. Some PT-CAs reported that they may suggest or decide on their own to create dedicated subCAs, branded or not, to distinguish from their general-purpose issuing CAs when servicing large customers or projects, as a means to isolate the impact/risks in case of an incident (e.g. compromise, compliance failure or other type) that necessitates revocation.
5. The vetting typically involves the following validation activities:

   a. verification of the organization’s name, address, and existence (similar to an OV or EV process); and

   b. verification of the authorization of the request.

6. One of the participating PT-CAs reported that, before signing a contract, an internal consultation takes place with the Compliance team to check the reputation of the branded SubCA Applicant. This includes searching public resources for reports of involvement in data falsification or money laundering activities. CCADB and Bugzilla are additional sources of information when an applicant is already a PT-CA itself.
7. None reported denying a branded subCA client for reasons other than commercial/financial.
8. Almost all PT-CAs reported that most branded subCAs bring their own user portal; one PT-CA quantified it to 80% of their total number of branded subCA partners. As an exception, one PT-CA was not aware of any of its branded subCA customers using their own user portal.
9. No PT-CA reported auditing or otherwise inspecting the third-party user portal of their branded subCAs (unless the branded subCA is also a PT-CA, which means their user portals are subject to audit anyway).
10. One PT-CA reported the following lessons learned:

    a. The number of issued certificates should be large enough to justify maintaining a branded subCA.

    b. It is worth checking their experience in the industry before proceeding with the contract.

c. It is also worth taking care of the appropriate length of the contract.

11. A couple of PT-CAs reported they don't see any particular technical challenges with generating, controlling, or revoking branded subCAs.

# Value Added Resellers

According to the results of the survey and the information we gathered with our own investigation, almost all PT-CAs offer reseller programs; from companies or individuals who enjoy wholesale discounts and resell CA products for a margin (plain resellers) to entities that incorporate CA products to their own offerings or provide value-added services to the benefit of their customers. The former ("plain resellers") are not involved in any part of the service other than the sale itself, therefore they are considered out-of-scope in this paper.

On the other hand, Value-Added Resellers (VAR) may have small or significant involvement in facilitating the key/certificate lifecycle process. Since this has security and compliance implications, this paper focuses on VARs and considers inherent risks (and benefits).

Our research revealed that there are different types/practices for VARs in the industry, depending on their involvement in the key/certificate lifecycle processes, the use of the PT-CA's portal or their own portal / systems, the use of subCAs issued with the name of the PT-CA/Root CA, or branded subCAs.

The most common cases we identified are the following:

- **VARs which utilize the PT-CA's/Root CA's systems**: They commonly assist the entities owning/controlling Domain Names by using the CA's Registration Authority Portal; their assistance is usually focused in the registration and management of certificates on behalf of these Domain owners.
- **VARs with independent Registration Authority Portals:** They typically have their own portal to register users independently of the CA and use the CA's API in the backend to perform Certificate Lifecycle activities.
    - Domain Validation activities are typically performed by the CA. For example, if an email message with a Random Value is to be sent to the Applicant to prove control of a Domain Name, it is sent directly from the PT-CA's systems, not the reseller's.
    - According to section 6.1.1.3 of the BRs, PT-CAs are not allowed to generate key pairs on behalf of Subscribers. Some Subscribers may use VARs to generate and possibly store those keys.
- **Branded subCA Resellers:** In most cases, these are VARs that have an agreement with the PT-CA to acquire a custom issuing CA that contains the "brand" of the VAR.
    - This is typically an **internally-operated subCA**, so the parent (usually Root) CA operator usually manages the keys and lifecycle events of that subCA.
    - **Externally-operated subCAs** may also contain the brand of the entity operating the subCA, but since this entity controls a Private Key associated with an Issuing CA Certificate, it must be properly audited according to section 8.1 of the TLS Baseline Requirement, or it must be technically constrained in line with sections 7.1.2.3, 7.1.2.4, 7.1.2.5 and internally audited according to section 8.7 of the TLS Baseline Requirements. It is considered out-of-scope in this white paper.

In addition to branded subCA Resellers, large-size Subscribers may also request a branded subCA to issue certificates under their organization name (i.e. for their own use). This model is not examined here because it has the same risks as with a simple Subscriber, in the sense of ordering and managing large volumes of certificates for their own their own Organization.

Similarly, resellers not involved in any part of the key/certificate lifecycle management (for example, resellers that are part of a referrer program with commissionable sales) are not in scope of this white paper.

# Branded SubCAs

Externally-operated subCAs, a model that was popular in the past (based on analysis of CCADB data) have been significantly reduced over the last years (in the CCADB, there were 93 serverAuth subCAs with “Audit not same as parent” still active and chained to a trusted Root), and continues to be used in some cases. When used, the subCA certificate includes the partner’s name in the organizationName of the subjectDN and requires separate external audits.

The industry uses two practices for the internally-operated branded subCA Organization:

- Some CAs include the Issuing CA (Root Operator) name in the organizationName of the subjectDN of the branded Intermediate CA Certificate
- Some CAs include the name of the branded SubCA in the organizationName of the subjectDN of the branded Intermediate CA Certificate.

With the current requirements, it is difficult for a Relying Party to easily identify whether the Issuing CA is **operated** by the Root CA or another entity.

# Risks of the VAR model

After analyzing the feedback from the survey and the various VAR practices in this industry, we identified some risks that are applicable mainly to VARs acting on behalf of a Subscriber:

1. **Key generation** and/or **storing** of the private key: This is a critical function for which no requirements or audits are enforced to VARs by the current standards. The lack of visibility to their security posture increases the risk of getting Subscriber’s private keys compromised.
2. **Storage of Personally Identifiable Information**, and possibly other sensitive (e.g. credit card) information, with the risk of private data exposure.This risk is similar to the one mentioned above; in addition, there is a risk of improper use of PII, i.e. use of PII for purposes other than the ones approved by the Subscriber.
3. **Certificate revocation**, with the Denial-of-Service risk to Subscribers. In the case of VARs that have privileged access to their customers’ accounts, an incident on a VAR’s system or even an accidental action by the VAR may result in bulk revocation, thus affecting the availability of multiple websites.
4. **Certificate re-key**, allowed in certain circumstances to replace a public key in a certificate without re-performing Domain Validation, with the risk of intercepting encrypted traffic to/from Subscriber websites.
5. **Re-use of evidence used for Domain Validation:** Upon initial issuance, there is a direct interaction with the domain owner that allows the PT-CA to have full control over the DCV process. In the case of DCV evidence re-use, this step is not applicable, which means there is a risk that the VAR may successfully request issuance of a new certificate to the domains in question without the Subscriber’s permission.

6. **VARs have increased impact and thus become a "honeypot" in case of compromise**. A VAR would be considered a more appealing target, and if an attacker successfully penetrates/compromises a VAR's systems (e.g. its portal), this could affect more independent Subscribers resulting in a much larger impact compared to attacks on individual Subscribers.
7. The use of a custom **reseller portal** adds one more element in the security chain, extending the attack surface. Specific risks to a reseller portal include:
    1. Cybersecurity threats
    2. Poor information security hygiene
    3. Weak Authentication/Authorization/Accounting mechanisms
8. Adding more people from the reseller's business to **privileged positions** of the certificate lifecycle management process leads to an increased attack surface.
9. **Malicious acts** by the VAR; this is inherent to any delegated activity where an entity acting on behalf of the real beneficiary of a service (in our case, the Certificate Subscriber), may act maliciously. A simple example would be a malicious VAR "assisting" an Applicant to generate a Key Pair and later selling the Private Key to an attacker.

During our analysis, we identified that if a VAR is granted an internally-operated branded subCA, the risks are the same, though conceptually the branded subCA is now considered "trustworthy" because the Root CA is essentially "vouching" for the subCA. Please note that CRL, OCSP, CAIssuer URLs also need to be internally-operated by the Root CA.

# Good Practices

After considering the above risks, we would like to suggest some good practices that can minimize the potential of any shortcomings or inappropriate actions by subCA customers.

**For branded subCAs:**

- **Know your potential partner**: Issuing a branded subCA certificate conceptually grants the reseller the reputation and trustworthiness of the PT-CA. Consequently, it is important for Root CA operators to vet their potential reseller, from identity validation (following OV/EV guidelines) to legal documentation to researching the company's reputation and the reputation of the owners and management team.
- **Re-verification and re-evaluation:** Periodic re-verification of all branded subCA resellers' business registrations should be applied to ensure legality and good standing. In addition to the use of public sources, re-evaluation of resellers may consider their performance during the ongoing partnership.
- **Contractual provisions and policies**: PT-CAs should make sure they maintain control over the contract, so that any contract termination and subCA revocation resulting from a contract breach is at their sole discretion. Branded subCA agreements could include provisions that give the PT-CA more visibility over the reseller's practices and set minimum requirements with regard to internal security, customer-service and adherence to the BRs (in case they are acting as a Delegated Third Parties).
- **Legal environment**: Considering the laws and customs of the jurisdiction where the reseller will be operating is necessary before granting a branded subCA to foreign entities. This may include compatibility of privacy laws and licensing requirements.
- **Maintain control of resources:** Some jurisdictions may require that only localized businesses operate in their area; this may include the ownership of domain names or key infrastructure. Some customers request 'extended' branding, e.g. branded OCSP responder URLs and other resources that are part of the PT-CA's obligations. The PT-CA must ensure

that its control over these resources shall survive from a possible termination of such an agreement, else it risks violation of CA/Browser Forum requirements.

- **Cost-benefit analysis and risk treatment**: The branded subCA model may be lucrative, but it also comes with compliance and reputation risks. A prudent PT-CA analyzes these before granting reputation and trustworthiness to a potential partner. In addition to just approval or rejection, the decision may include controls that remediate any risks identified.
- **Transparency**: Through branding, resellers (may wish to) promote themselves as “publicly-trusted CAs”. Transparency dictates that consumers and relying parties have at least an indication of the actual entity they put their trust to. One suggested way is to keep the third-party’s name in the *commonName* of the *subjectDN* of the branded subCA certificate and use the organization name of the actual CA Operator (e.g. the PT-CA) in the *organizationName*.

**For all VARs:**

- **Security measures**: For VARs, SSL.com has issued the “Certificate Authority Security Best Practices Guide for Branded Resellers: Comprehensive Security Measures”. It includes a comprehensive series of possible security measures and references to NetSec Requirements. In the simplest case that a VAR is not using their own systems (e.g. user portal) for the certificate lifecycle, some of the requirements may not be applicable.
- **Protection of subscribers**: PT-CAs should identify and address the risks associated with system access made available to VARs. A PT-CA should have different access levels for reseller and non-reseller accounts, enabling more restrictions on the reseller access level to protect Subscriber accounts from abuse. For example, this may include controls to prevent re-use of previous Domain Validation evidence by VARs. To this end, Baseline Requirements could also require that anyone who isn't an 'Enterprise RA' (i.e. requesting just for their own, owned orgs and domains) must complete Domain Validation for every issuance (issue, reissue, rekey, duplicate, and renewal).
- **Subscriber and reseller agreements**: PT-CAs could offer two types of Subscriber Agreements: a Subscriber Agreement that does not allow reselling and a Dedicated Reseller Agreement that contains extra clauses and expectations For example, Reseller Agreements could include provisions related to the management of Subscriber accounts and promote information security sanitization as described in the Certificate Authority Security Best Practices Guide for Branded Resellers: Comprehensive Security Measures. **For VARs with their own portal:**

Note: We do not consider the case of a hosting provider who participates in the certificate lifecycle, typically in an automated manner via common web hosting control panels (Plesk, VirtualMin, CPanel).

- **Contractual provisions and policies**: Include additional provisions to the Reseller Agreement, such as the right to audit, suggest/require annual penetration testing, review of system configurations, implement MFA or authentication controls at least at the same level as the PT-CA, monitoring and incident disclosure.
- **Secure integration**: Enforce the use of secure APIs, for example apply secure authentication via encrypted channel, limited session duration, proper scoping to the accounts/records affecting only the VAR and its customers/Subscribers, etc.
- **Vulnerability management**: Ensure periodical vulnerability scans are conducted against the reseller portal. This may be required by the Reseller Agreement or may be part of the services offered by the PT-CA to assist in the good security hygiene of the reseller’s portal.

- **Evaluation of their security posture:** Collection of security-related information and risk evaluation as part of the reseller onboarding process. This can be applied using structured questionnaires or specialized software.
- **Annual Evaluation:** PT-CAs should not just set up unmonitored VAR relationships. It is important to implement an evaluation process that is conducted at least on an annual basis.
- **Awareness newsletters**: Sending periodic security awareness newsletters helps resellers to improve their understanding of cybersecurity threats and be better prepared against attacks. These newsletters could contain information about any new security warnings related to PKI systems, a tally of attempted (or successful) attacks, or instructions on how to engage the tools and techniques needed to improve security hygiene.

# Conclusions

Just like any opportunity, the sale of branded subCAs has both positive and negative aspects. More so than the sale of end-entity certificates, branded subCAs open the trusted CA to potential harm based on the activities of the reseller-client, while still offering the potential of great benefits. VARs should not be overlooked though; their business and security practices may introduce risks to subscribers and thus to the reputation and trustworthiness of the PT-CA.

Before entering into any branded subCA or VAR relationship, PT-CAs are cautioned to conduct thorough due diligence, consider all potential ramifications, take informed decisions, and enter into well-developed contracts that are protective of the PT-CA's trust. This paper shows there are options available, there are lessons learned, and there are good practices to follow.