



🌐 **Farsi Version** →

📄 **Download PDF** .PDF

🔍 **Accessibility**

Text Size — 100% +

Investigations

When the Chain of Trust Breaks Certificate Revocations, Sanctions, and the Risks of “Nationalizing Trust” on Iran’s Internet

📅 October 8, 2026 👤 Solmaz Eikder

Related Articles

- 1 Examining the Impact of Filtering on Small and Medium Enterprises:
- 2 Ebrahim Raisi’s Enduring Impact on the Internet: A Legacy of Destruction
- 3 Iran’s Nazer App Aims to Expand State Surveillance and Control
- 4 Technology as a Tool for Repression: A Network of Telegram Channels Promoting Sexual Violence and Suppression of Dissent
- 5 A Review of Digital Freedom Violations on the Second Anniversary of the Mahsa Amini Movement: Digital Iran Bound by Policy and Restrictions

When a user in Iran attempts to access a banking website and their browser displays the warning “Your connection is not private,” the problem is not simply that the webpage has failed to load. The warning means the browser cannot reliably verify that the website actually belongs to the bank it claims to represent. Recent problems with website security certificates in Iran, affecting institutions from the Central Bank of Iran to the country’s electronic payment network, Shaparak, show how Iranian users’ secure access to essential services has become dependent on the decisions of foreign companies, commercial intermediaries, and domestic authorities.

The Central Bank’s experience also demonstrates that replacing Western providers with a Chinese certificate issuer is not necessarily a sustainable solution. A certificate issued through the chain of the Chinese company TrustAsia was revoked before its scheduled expiration date. For users, the consequences of this instability include a heightened risk of phishing, repeated domain changes, the normalization of browser security warnings, and mounting pressure to trust a domestic root certificate authority whose scope of authority, auditing standards, and accountability mechanisms have not been adequately disclosed.

- 6 The Monopoly of Internet Infrastructure in Iran: Challenges and Consequences of Restrictions on Access and Cybersecurity
- 7 SIM Card Deactivation: A Pilot Scheme for Widespread Citizen Suppression
- 8 Open Technology Fund’s Security Lab Finds Three Widely Used Iranian Messaging Apps Are Not Safe

What Is SSL, and Why Does It Matter?

The term SSL remains common in public discussion, although the technology currently in use is more accurately called TLS. A TLS certificate can be understood as a website’s digital identity document. It links a domain name to a cryptographic key and allows the browser to answer several essential questions:

- Was the certificate issued for this specific domain?
- Is it still within its validity period?
- Which certificate authority issued it?
- Does the browser trust that certificate authority?
- Has the certificate been revoked before its expiration date?

If these checks are successful, the browser establishes an encrypted connection. Under normal conditions, parties positioned between the user and the website should not be able to easily read or alter the information being exchanged. At the same time, the certificate helps the browser confirm that the user is communicating with the same domain displayed in the address bar.

This identity-verification function is particularly important in online banking. Users submit sensitive information such as usernames, passwords, card numbers, CVV2 codes, and one-time passwords on banking and payment pages. Encryption alone is insufficient: a connection may be encrypted while the server at the other end is controlled by an attacker. This is why browsers interrupt the connection or display a prominent warning when they cannot verify the destination’s identity.

An invalid certificate does not necessarily mean that all data is being transmitted without encryption. More precisely, it means the browser cannot authenticate the other party through the conventional chain of trust. For a financial service, that uncertainty alone should be sufficient reason not to submit sensitive information.

From the Central Bank’s Announcement to a Verifiable Revocation

On August 15, 2026 (24 Mordad 1405), the Central Bank of Iran [announced](#) that the security certificates of several websites associated with the institution had been revoked by a “foreign provider.” The announcement did not identify the provider, the affected domains, the certificate serial numbers, or the official reason for the revocations.

For one certificate covering the Central Bank’s domains, however, there is [publicly verifiable evidence](#). The certificate covered `cbi.ir` and `*.cbi.ir` and was issued through the LiteSSL chain associated with TrustAsia. Its validity period was scheduled to run from July 27, 2026, to February 11, 2027. It was revoked on August 10, several months before its scheduled expiration. The

issuer’s Certificate Revocation List recorded the reason as privilegeWithdrawn, indicating that a privilege or authorization associated with the certificate had been withdrawn.

Chinese Providers Also Revoke Iranian Certificates

TrustAsia is a Chinese company based in Shanghai, and its name appears in the certificate issuance records of several Iranian banks. As access to some Western providers became more difficult, Iranian banks’ reliance on a Chinese company may have created the impression that China could offer a stable alternative independent of US sanctions. The revocation of the Central Bank’s certificate demonstrated that this assumption is not reliable.

A company’s Chinese ownership does not make it independent of the global WebPKI ecosystem. For TrustAsia certificates to be accepted without warnings by Chrome, Firefox, Safari, Android, or Windows, their chains must terminate at roots trusted by these products and comply with root-program requirements and industry standards. This dependence exposes the company to the rules and risk assessments of the global market.

Chinese companies may also comply with US sanctions even when they are not directly required to do so, in order to preserve banking relationships, maintain access to international markets, or reduce commercial risk. A knowledgeable source who spoke to Filterwatch on condition of anonymity said that Chinese companies do, in practice, comply with US sanctions against Iran. This account is consistent with the TrustAsia revocation, but it does not replace an official explanation from the issuer regarding the specific Central Bank certificate.

Public data also show that TrustAsia has issued certificates for domains associated with Bank Melli, Bank Mellat, Bank Sepah, Bank Tejarat, Bank Refah, Post Bank, Bank Maskan, and several private banks. The appearance of a certificate in public records does not by itself prove that it is currently installed on a bank’s production service. Nevertheless, TrustAsia’s extensive presence indicates that China has become an important certificate-supply route for Iran’s banking network.

The short answer to the question “Can China replace the West?” is therefore no. China may provide a temporary alternative route, but the Central Bank certificate revocation shows that this route is not insulated from international legal and commercial pressures.

Shaparak: When the Crisis Reaches the Payment Page

In October 2026, reports emerged that a wildcard certificate covering *.shaparak.ir had been revoked. The certificate associated with these reports was issued by SSL.com and was not scheduled to expire for several more months. Public records establish that the certificate was issued, but without a signed OCSP response, a corresponding CRL entry, or an official

explanation from SSL.com, the reported revocation cannot be conclusively attributed to sanctions.

Shaparak is particularly important because subdomains of shaparak.ir are used by payment service providers for online payment pages. Users enter card numbers, expiration dates, CVV2 codes, and dynamic one-time passwords on these pages. If a payment page presents an invalid certificate, a browser or application may terminate the connection. If users are encouraged to bypass the warning, the risk becomes more serious: a fraudulent domain can exploit the resulting confusion to steal payment information.

Certificate Transparency records show that, over a short period, certificates for *.shaparak.ir were obtained from several issuers, including Actalis, Let’s Encrypt, TrustAsia, and SSL.com. Maintaining certificates from multiple providers is not necessarily a security failure; it may form part of a contingency plan. Nevertheless, the rapid movement between issuers suggests that stable access to a publicly trusted certificate chain has become a serious concern.

Direct Risks to Iranian Users

- **Increased phishing:** Repeated changes to banking and payment domains make official addresses harder to recognize and make fraudulent “new bank address” messages more convincing. A padlock icon alone does not prove that a website belongs to a bank.
- **Normalization of browser warnings:** Encouraging users to bypass certificate warnings weakens an important safeguard before sensitive information is submitted and increases the likelihood that users will also ignore warnings on fraudulent websites.
- **Disruption of banking and payments:** An invalid certificate can make online banking, mobile banking, and payment pages inaccessible or leave the status of a transaction unclear.
- **Failure of backend communications:** Connections among banks, merchants, payment companies, identity services, and cloud systems may also fail, even when the public-facing website appears to remain available.
- **Costs for businesses:** A domain change may require businesses to update their e-commerce trust seal, licenses, payment gateway registration, links, and advertising campaigns.
- **Dependence on domestic tools:** Instability in foreign certificate services may turn the use of a domestic browser, a specific application, or a locally issued root certificate into a condition for accessing essential services.

A Domestic Root Certificate: Service Continuity or Centralized Trust?

As foreign certificate providers become less reliable, Iranian authorities have increasingly turned to domestic alternatives to maintain access to essential online services. According to a [report](#) by Peivast, the Central Bank instructed the banking network to use Iran’s domestic root certificate infrastructure, and at least eleven banks entered the process of obtaining locally issued certificates. Domestic certificates can use standard algorithms and strong encryption. The central problem, however, is that widely used browsers and operating systems do not automatically recognize or trust Iran’s root certificate authority.

To address this limitation, users may be instructed to install the root certificate on their devices or use a browser in which the root is already trusted. Installing a root certificate is fundamentally different from installing a certificate for a single website. A website certificate applies to a particular domain, whereas a trusted root may validate certificates issued for many domains. If such a root is installed at the operating-system level, applications and browsers that rely on the system trust store may accept certificate chains issued beneath it.

This capability does not, by itself, prove surveillance or abuse. Many countries and organizations operate internal public-key infrastructures. The risk increases when the root’s scope of authority, key-management practices, issuance procedures, domain restrictions, independent audits, public logging, and incident-response mechanisms are not transparent to users and outside researchers.

If a trusted root’s private key is stolen, if a certificate is issued incorrectly, or if the authority is abused, impersonating websites and interfering with users’ communications may become technically possible. The more devices on which the root is installed, the wider the potential impact.

How Sanctions Contribute to the “Nationalization of Trust”

The shift toward domestic certificate infrastructure illustrates a broader problem: foreign sanctions and Iran’s domestic internet-control policies, while not necessarily coordinated, can produce outcomes that reinforce one another. When a foreign provider restricts a service because of sanctions, overcompliance, or a commercial decision, an Iranian organization may respond by moving its domain, hosting, security certificates, or software to a domestic alternative to maintain access. As a result, essential online services become increasingly dependent on infrastructure controlled inside Iran.

The TrustAsia experience shows that shifting from Western providers to Chinese companies does not eliminate this dependence. Chinese companies also operate in global markets and may incorporate similar legal and commercial considerations into their decisions. An Iranian organization

may therefore conclude that building a domestic chain of trust is the only reliable long-term option.

The benefit of this approach is service continuity when a foreign certificate authority terminates cooperation. The cost is the transfer of trust from the public WebPKI ecosystem to a domestic institution about whose issuance policies, independent audits, and accountability mechanisms less public information is available. If access depends on installing a root certificate or using a designated browser, the issue becomes directly connected to user choice and informed consent.

An Example Beyond Certificates: Disruption in Google Account Creation

The risks of relying on foreign digital services extend beyond security certificates, as recent difficulties accessing Google services in Iran illustrate. In September and October 2026, some Iranian users reported that phone numbers with the +98 country code were rejected during Google Account creation or recovery, or that verification messages never arrived. Google’s official [guidance](#) states that phone verification is required only in certain circumstances to confirm that a user is a real person and to prevent bulk account creation and abuse. Google has not announced a blanket ban on Gmail account creation for Iranian users. The problem therefore cannot conclusively be described as a “Gmail sanction.”

The service does not behave identically for all users. In the cases examined for this report, an account could be created without phone verification on a device that already had a history of using a Google Account. On a browser or device without such a history, however, phone verification became mandatory and the Iranian number was rejected. This difference suggests that device history, IP address, cookies, VPN use, and Google’s risk-assessment systems may influence the decision.

The precise cause remains unknown. If a number is immediately rejected with the message “This phone number cannot be used for verification,” the decision was probably made by Google’s anti-abuse system or an identity-verification contractor before any message was sent. If the number is accepted but the message never arrives, the problem may lie with an SMS intermediary, an international telecommunications route, or an Iranian mobile operator. Without an official response from Google and access to message-delivery records, the point of failure cannot be determined.

The consequences extend beyond the inability to create a Gmail address. A Google Account is used to activate many Android functions, download applications from Google Play, access Google Drive and Photos, back up devices, and sign in to third-party services. Verification problems may also make it difficult to recover existing accounts. A restriction whose cause and responsible party remain unclear could therefore exclude Iranian users from

parts of Google’s ecosystem and make domestic services the only practical alternative.

Tags **Browser Security Warnings**

Domestic Root Certificate Authority

Google Account Access Issues

Phishing

Security Certificate Revocation

SSL/TLS

↓ **Google**

فارسی
filter.v

