ZERO TRUST

As a rule, no user or device is to be trusted - regardless of whether it is internal or external. Access is only permitted after strict authentication and access control. Communication with other network participants (human or technical) only takes place with the appropriate authorisation.

PUBLIC TRUST

Publicly accessible services such as websites or social media platforms that are available to the general public. Most users and devices are allowed access without strict access control or authentication.

PRIVATE TRUST

Trust is only granted to specific, internal networks or user groups. Access is restricted to sources authenticated by security measures such as firewalls. Unknown and external users or devices are blocked.

6,400

There are 6,400 Google queries around the topic of Zero Trust within one month.

15 MRD.

It is estimated that 15 billion IoT devices will be in use worldwide by 2023. Which one can you trust?

It's time for Zero Trust.

Move forward with essendi xc.

How many identities do you actually have in your network?

XC AND ZERO TRUST

In a Zero Trust environment, a reliable tool for authentication is necessary. To identify yourself to a Zero Trust system, you need a "badge": a digital certificate. As a fully comprehensive certificate management tool, essendi xc issues digital certificates automatically according to defined compliance specifications and distributes them to the target systems. It is thus an essential cornerstone for secure and smooth communication in zero-trust environments.

EU contact	essendi it GmbH, Dolanallee 19, DE-74523 Schwäbisch Hall	☎ +49 791 943 07 011	✉ xc@essendi.de	xc.essendi.it
International contact	essendi it AG, Bahnhofplatz 1, CH-6460 Altdorf, UR	☎ +41 41 874 27 30	✉ xc@essendi.ch	xc.essendi.it