# Factor

02.05.2025 14:29:04

**FAQ-Artikel-Ausdruck**

| | | | |
|---|---|---|---|
| **Kategorie:** | RRZE: Glossary | **Bewertungen:** | 0 |
| **Status:** | öffentlich (Alle) | **Ergebnis:** | 0.00 % |
| **Sprache:** | en | **Letzte Aktualisierung:** | 11:54:04 - 28.06.2010 |

***Schlüsselwörter***

identity, security

***Symptom (öffentlich)***

***Problem (öffentlich)***

***Lösung (öffentlich)***

The fundamental classification of credential types. There are actually only three factors: what you "know", what you "have", and what you "are". Combining two, or three, into a multiple-factor solution is a means of stronger authentication ["https://www.rrze.wiki.uni-erlangen.de/index.php/Glossar#Authentication"]. There are suggestions from time to time of new factor classifications such as "what you do" or "where you are", but they always resolve into the basic three.

Recent suggestions have included Context-based access (or Presence), which attempts to assign access rights based on the platform or the location of the user; but these are simply something you "have". Examples are a particular PC configuration, IP address, MAC address or a Device-id. This is not to say that context inicators (such as when, where, how) can't be used in an authentication framework; they can, but mostly as an inicator that the identity is not using the usual device based on past patterns, weaking the original assurance level (therefore requiring further challenges), or causing the provider to use a different assurance-framework instance that requiries a different challenge (or via a different channel) . IP address can also be used as a blocker to services where government regulations prevent access, and as a check to prevent session piggybacking, but it is not really a 'credential'.

Also the idea of Reputation is occasionally suggested as an identity or as a credential; but it is only a temporary trust attribute that may only be valid for a single session and as such is not an integral part of the identity. Examples are an eBay sellers rating or history, a criminal record, a reference check, a credit report. These can still be considered as part of the risk/trust relationship to determine what accesses you have or are permitted to do in a session, but they are not really an authentication credential and therefore not a credential type or factor.

Another recent idea is "who you know"; clearly this is simply what you know about an identity and therefore is not a new fourth factor. More importantly "who you know" can have little or no value as a credential in an assertion unless it relies on proving that claim, and that must include the identity that you know confirming that they know you. Perhaps "who knows you" might be useful in establishing an identity but that is a Registration strength, not a Credential strength - refer to Known Customer, and Assurance Framework

Similarly, using multiple challenges such as several passwords or secret question/answer sets is not multi-factor - it is only multiple tiers of the same factor (more things that you "know"). No matter how many you use, the added strength of each SQA adds an exponentially smaller increment. It can't increase the assurance level to equate the strength of two factors, although it can go close.

Source: "http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html"