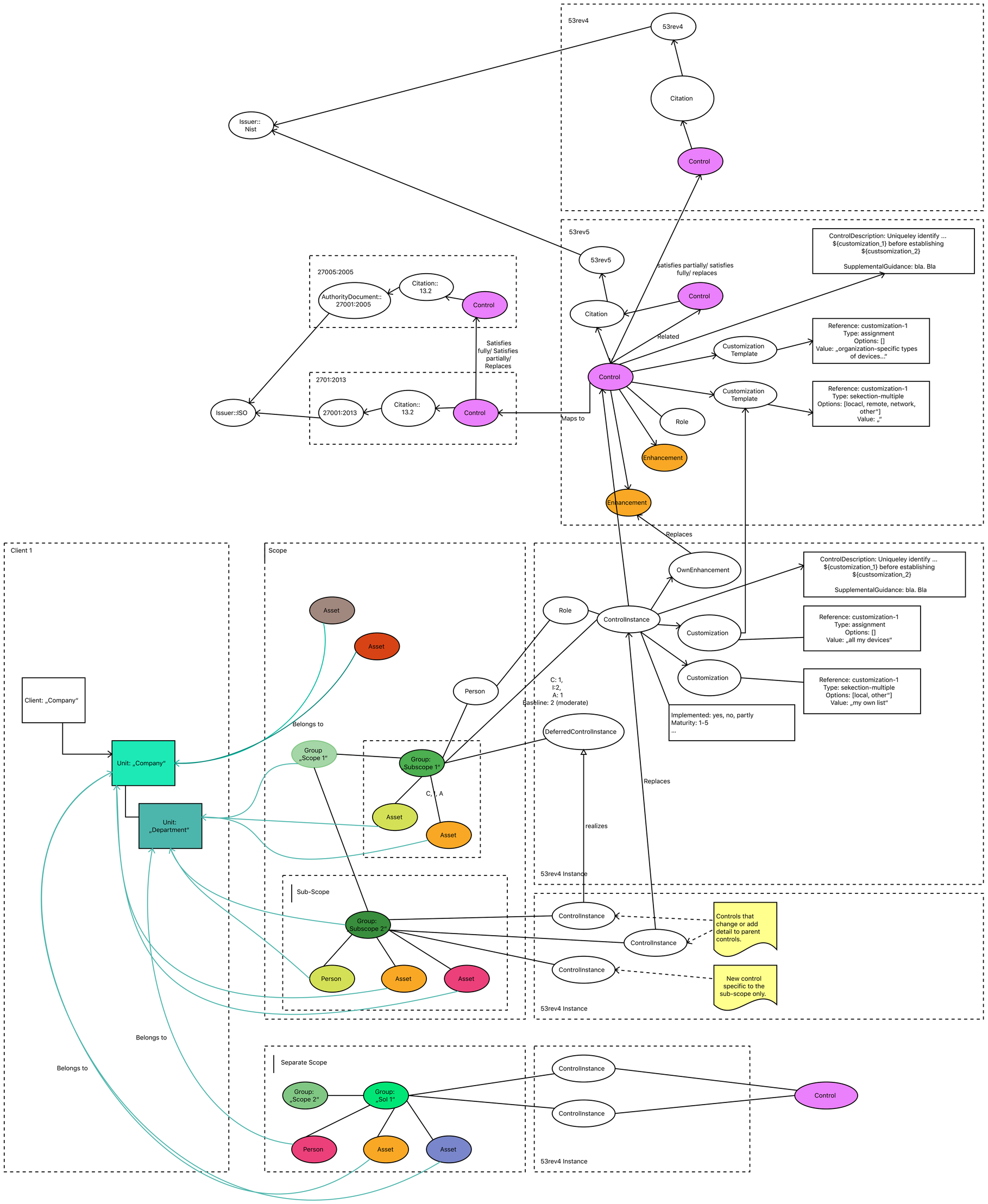

Everything in the catalog packages is a VALUE OBJECT.
Control here has no identity. It doesn`t matter which control you receive from an authority document.

Anmerkungen machen Bearbeiten

NIST SP

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

Supplemental Guidance: ~~Organizational devices requiring unique~~ device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

Control Enhancements:

(1) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*

The information system authenticates [*Assignment: organization-defined specific devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.

Supplemental Guidance: A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). Related controls: SC-8, SC-12, SC-13.

(2) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*

[Withdrawn: Incorporated into IA-3 (1)].

(3) *DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*

The organization:

(a) Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and

(b) Audits lease information when assigned to a device.